CWID 2006 FINAL REPORT

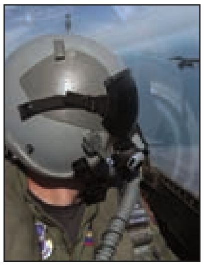
Assessment Briefs Contents

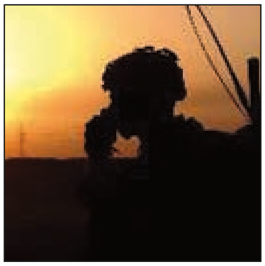
PAGE	TITLE: DESCRIPTION
3	Executive Summary: Overview of demonstration execution, June 2006
5	CWID 2006 Top Performing Technical Solutions: List of outstanding trials
6	Analysts, Agencies Collect Data: Assessment process overview
8	CWID, Connecting the Globe: Network engineering overview
10	NATO Leverages CWID Forum: A multinational perspective
13	Interoperability Trials: Contents of trials summary section followed by briefs on each trial
32	History of CWID
	Inside back cover: Acronyms and Abbreviations

OPEN BOOKMARKS
GO TO CD TRIAL DIRECTORY
GO TO CD HOME PAGE

Published by: CWID JMO DISA
Edited by: CWID JMO Hampton, VA
For information or to obtain copies, contact: CWIDPA@langley.af.mil
www.cwid.js.mil

NOTES





CWID 2006 FINAL REPORT ASSESSMENT BRIEFS

Executive Summary

The Coalition Warrior Interoperability Demonstration (CWID) is a Chairman of the Joint Chiefs of Staff annual event that features Interoperability Trials (ITs) focused on selected core objectives defined by combatant commanders. ITs approved for participation were required to provide a new capability or improve on an existing capability in support of the 2006 objectives.

The demonstration tested and evaluated technologies and capabilities for exchanging information among agencies, services and this year's host combatant commander, U.S. European Command (USEUCOM).

CWID 2006 enabled USEUCOM, United States Northern Command (USNORTHCOM) and the international community to investigate command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) solutions that focused on relevant and timely objectives for enhancing coalition interoperability. The coalition interoperability effort sought solutions applicable in the operational community and that enabled a standard procedure for information sharing between coalition partners.

THIS YEAR'S IT CAPABILITIES were examined through a challenging two part scenario: one part for the Combined Task Force (CTF) and one part for Homeland Security and Homeland Defense (HLS/HLD). For the CTF portion, CWID provided a framework that facilitated IT participation through a full range of military operations conducted by U.S. and coalition forces. CTF operations were set in a notional context in scripted countries.

The HLS/HLD portion consisted of federal, state and local agencies responding to terrorist attacks and natural disasters within the U.S. Simulated attacks were tied to conventional CTF operations on another continent.

The host site for this year's CWID execution period was USEUCOM, Kelley Barracks, Stuttgart, Germany, but visitors experienced operations and interoperability trials at more than 25 sites around the world.

U.S. VISITOR SITES included: USNORTHCOM HLS/HLD in Colorado Springs, CO; the U.S. Army, U.S. Marine Corps and National Guard Bureau at Naval Surface Warfare Center, Dahlgren Division (NSWCDD), VA; the U.S. Navy at Space and Naval Warfare Systems Command (SPAWAR), San Diego, CA; and the U.S. Air Force at Electronic Systems Center (ESC), Hanscom AFB, MA. Global network sites included Australia, Canada, New Zealand, United Kingdom,

2006 OBJECTIVES

1. COALITION COMMAND & CONTROL (C2): Enhance the Commander's Coalition C2 capability through secure, scalable and bandwidth sensitive technologies, within and between communities of interest (COIs) and information domains of differing security classifications.

2. COALITION INFORMATION SHARING: Provide solutions that improve the Commander's ability to share information within a multi-lingual coalition that is secure, scalable and bandwidth sensitive. Included in this objective are improvements to language translation tools that provide grammatically correct, militarily appropriate context, multi-language translations to support verbal and textual collaboration within and between disparate information domains.

3. INTEGRATED LOGISTICS: Provide solutions for responsive, effective logistics within and between multiple information communities of interest (COIs).

4. CONTINUITY OF OPERATIONS: Provide C2 solutions that enhance the Commander's ability to plan, communicate and affect coalition operations while remotely deployed. Inherent in this objective is the ability of the commander to maintain situational awareness and connectivity with subordinate activities while en route to the theater in crisis.

5. NET CENTRIC ENTERPRISE SERVICES: Provide solutions that enhance the Commander's ability to collaborate and disseminate information among communities of interest (COIs) in a Net Centric environment.

and other NATO nations.

Thirty-Four ITs participated in the two-week CWID execution period held from 12-22 June. In preparation for the event, trials, their sponsors and the CWID Joint Management Office (JMO) support staff created a Master Scenario Events List (MSEL) containing more than 2,700 events. Over 400 operators from the military and supporting agencies, at multiple U.S. and coalition sites, used the MSEL events to execute the CWID 2006 scenario and evaluate each trial's performance.

CWID Dahlgren, VA, site

IT ASSESSMENT SUMMARIES documented in the following pages provide a brief overview of each trial's performance and complement detailed assessment data contained on the companion Compact Disk (CD), located on the inside front cover of this booklet.

USNORTHCOM complimented the CWID technology demonstration scripted scenario with a real-time first-responder exercise. Military and civilian police cooperated during the simulation to evaluate four current CWID technologies and two other technologies of interest to the command.

The HLS/HLD scenario described an aircraft hijacking on a flight from Boston, MA, to Los Angeles, CA. The Colorado Springs Police Department (CSPD) worked with Peterson Air Force Base's 21st Space Wing Security Forces to overcome hijackers after the aircrew diverted the jet to Colorado Springs Airport, Colorado Springs, CO. The exercise employed an actual civilian aircraft on the tarmac and CSPD's Command and Control Vehicle and Mobile Bomb Vehicle, both acquired through Department of Homeland Security grants.

Responders used new information sharing technologies to integrate communications, providing situational awareness and coordinated planning and control. Military and civilian teams isolated the area at the civilian field and breached the aircraft, quickly regaining control and placing scenario "bad guys" in custody.

FROM THE OTHER SIDE OF THE CONTINENT, CWID's Dahlgren, VA, demonstration site provided initial intelligence on the hijacking and subsequent surveillance and situational awareness as the operation unfolded.

The U.S. Marine Corps, represented at Dahlgren, is already acquiring technologies employed in USNORTHCOM's Colorado Springs exercise. Dahlgren's local sheriff's department expressed interest in scenario technologies while observing hijacking operations and other CWID demonstrations.

The live exercise within the CWID demonstration provided a venue to use information sharing tools that could assist federal, state and local authorities with command and control interoperability issues as well as providing on-the-ground situational awareness for the Global War on Terrorism.

FROM U.S. JOINT FORCES COMMAND

CWID 2006 Top Performing Technical Solutions

The interoperability trials (ITs) below are top performing technology demonstrations as recommended by the CWID Senior Management Group (SMG) and based on input received from participating warfighters/operators, the Network Operations Working Group (NOWG), the Systems Engineering and Integration Working Group (SEIWG) and site managers.

NOTE: Trials are listed in order of trial number.

U.S. CWID IT STANDOUTS

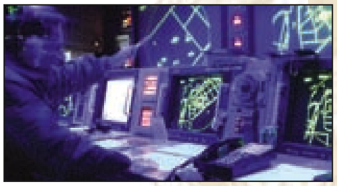
Trial No.	Title (Acronym)	Sponsor
IT01.20	Integrated Information Management System (IIMS)	USAF/AFRL
IT01.39	First Responder Interoperable Communications	USNORTHCOM
IT01.53	Coalition & Civil Agency Capable Wireless Information Transfer System (C3WITS)	USN/SPAWAR
IT03.09	Document Access Servelet (DAS)	USEUCOM
IT03.16	Intelligent Road/Rail Information Server (IRRIS)	US Army
IT04.03	Wide Area Interoperability System (WAIS) & ACU 1000	USNORTHCOM
IT05.06	Visualization for Information Assurance (VIA)	USAF
IT05.17	WMD Collaborative Advisory Response Systems (WMDCARS)	DTRA
IT05.37	Joint Effects Based C2 (JEBC2)	USNORTHCOM
IT05.47	HLS/HLD Collaborative Info Exchange Environment (CIEE)	NGB
IT05.52	Rapid Triage Medical Workbench (RTMW)	USNORTHCOM
IT05.66	Coalition Shared Information Environment (COSINE)	NATO/ACT

COALITION CWID IT STANDOUTS

ITs described below represent coalition-sponsored submissions demonstrated at U.S. sites or having received U.S. assessment at an execution site outside the United States.

Trial No.	Title (Acronym)	Sponsor
IT01.01	Northern European Command – C2 Information System (NEC CIS)	Denmark
IT01.34	Mobile Real-Time Radiological Surveillance Net (MobRadNet)	Canada
IT01.62	Mobile Forces Solution (MOFS)	Germany

GO TO CD HOME PAGE



THE ASSESSMENT PROCESS

Analysts, Agencies Collect Data

In accordance with the Chairman, Joint Chief of Staff Instruction (CJCSI), the Assessment Working Group (AWG) provides the Joint Staff, Combatant Commands/Services/Agencies (C/S/A), and other interested parties with an objective assessment of qualifying Interoperability Trials (ITs) with respect to warfighter/operator utility, interoperability and Information Assurance (IA).

THE ASSESSMENT PROCESS

The ultimate goal of the assessment effort in 2006 was to identify those trials that were the best candidates to provide solutions or enhancements to Command, Control, Communications and Computers (C4) interoperability challenges facing Joint, Coalition, Homeland Security (HLS) and Homeland Defense (HLD) operations in the near term, while protecting data and integrity on operational networks. The AWG organization was comprised of three separate analyst teams that provided three different categories of assessments:

- Warfighter/Operator Utility
- Interoperability/Technical
- Information Assurance

The ultimate goal of the assessment effort in 2006 was to identify those trials that were the best candidates to provide solutions or enhancements to C4 interoperability challenges...

These analyst teams were comprised of representatives from the Coalition Warrior Interoperability Demonstration Joint Management Office (CWID JMO), Joint Interoperability Test Command (JITC), National Security Agency (NSA) and Coalition nations. During the CWID planning/preparation phase, each analyst team scrutinized ITs, based on predefined criteria, to determine the level of assessment that could be performed. Each trial had the potential to receive any combination of the three assessment types or none at all. The CWID Senior Management Group (SMG) was responsible for prioritizing the participating ITs. The AWG considered this prioritized IT list, along with the specific nature of each trial, varied maturity level, and the AWG's maximum assessment constraint to determine the categories of assessment for which a trial qualified. For trials that did not qualify for a formal assessment during CWID, the AWG coordinated with the Systems Engineering and Integration Working Group (SEIWG) to ensure that a summary report was provided (when applicable). This summary report documents the results of the activities performed, and the testing conducted, during CWID execution.

Prior to CWID execution, AWG representatives highlighted problem/issues and any corrective actions for each IT through observations and interviews. This information, along with firsthand warfighter/operator input collected through the Joint Systems Integration Command (JSIC) Data Collection and Analysis Tool (JDCAT), and the results of their advertised data exchanges captured within the Web Information Services

Environment (WISE) Interoperability Collection and Assessment Tool (WICAT), were consolidated with the Information Assurance test results to complete the CWID assessment final report for each qualifying trial. The final assessment report highlights IT performance with regard to meeting original stated objectives, as well as findings from the Warfighter/Operator Utility, Interoperability, and Information Assurance assessments. This year, enhanced cooperation across all U.S. and coalition assessment activities increased the validity of the assessment process.

WARFIGHTER/OPERATOR UTILITY

The warfighter/operator assessment focused on "value added" to warfighters/operators, trial technical performance, and ability to meet objectives and capabilities in the CWID operational environment. During CWID execution, warfighters/operators and staff personnel operated and interacted with trials, evaluating system utility by completing CWID network accessible questionnaires generated via JDCAT. Questionnaires were developed for each trial based on:

- CWID objective/sub-objectives
- Predefined Master Scenario Events List (MSEL) events and/or definitive test schedules
- Trial capabilities
- Applicable Measures of Performance (MOPs) tailored to each trial

INTEROPERABILITY ASSESSMENT

The Interoperability/Technical assessment focused on trial's ability to exchange usable data with CWID network core/component services or other trials. Prior to execution, JITC worked with each trial's staff expert to define the system interfaces to be exercised and how these interfaces and anticipated data exchanges mapped to CWID objectives. Definitions were developed into information exchange requirements (IERs):

- What information is exchanged
- Who exchanges the information
- Why the information is necessary
- How the exchanges take place

During execution, the Interoperability Assessment team observed predetermined exchanges, ensuring that data transferred was received and processed correctly by the receiving system. Results were documented in the WICAT database developed by JITC. All information collected by JITC can be applied to the formal U.S. interoperability certification process, leading to faster development of emerging technologies.

The Assessment Working Group is comprised of three separate analyst teams that provide three different categories of assessments:

■

Warfighter/Operator Utility

■

Interoperability/Technical

■

Information Assurance

INFORMATION ASSURANCE ASSESSMENT

Information assurance assessment focused on how a trial counters identified threats and enforces identified policies consistent with appropriate usage assumptions for the projected warfighting environment.

Security Environment Elements are:

- Threats
- Assumptions
- Policies

Each assessed trial was documented for how well it countered environmental threats and enforced the environmental policies consistent with the assumptions for how the capability was intended for use. Threats and policies that were adequately addressed by the trial were identified as "security coverage." Threats and policies not adequately addressed by the trial were a "security exposure." Security exposures that could not be addressed by other elements represented "residual risks" that must be managed for a successful deployment.

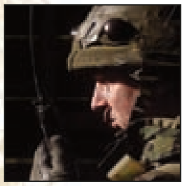
The information assurance assessment process contained three major phases:

- PHASE ONE occurred throughout the planning process and resulted in the documentation of functional flow, threats, and mitigation activities for each trial.
- PHASE TWO consisted of basic security tests performed during CWID execution to confirm the proper implementation of the mitigation activities.
- IN THE FINAL PHASE, selected Information Assurance related ITs get assistance from IA analysts developing documentation facilitating a formal evaluation through Common Criteria Testing Laboratory.

CWID EXECUTION

During CWID execution, AWG members were present at and collected assessment data from USEUCOM, four U.S. sites, and coalition sites in Australia, Canada, NATO, New Zealand and the United Kingdom.

Thirty-Four trials participated in CWID 2006. Of these, 32 received various levels of assessment from the three pronged warfighter/operator, interoperability and Information Assurance assessment process. Specifically: 30 trials received a Warfighter assessment, 29 received an Interoperability assessment and 10 received an Information Assurance assessment. SEIWG reported on five trials, two of which were not formally assessed by the AWG.



NETWORK ENGINEERING SUMMARY

CWID, Connecting the Globe

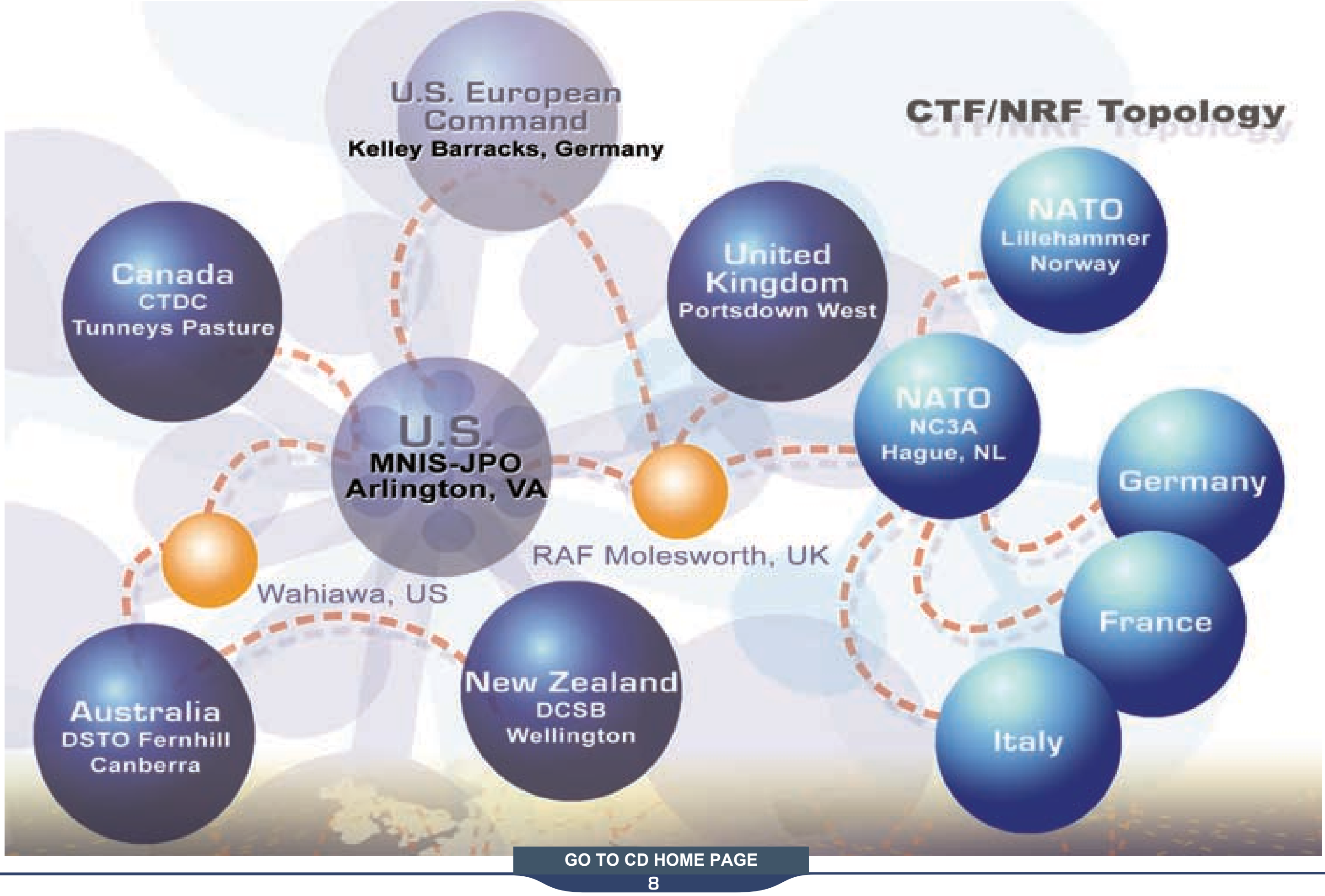
Over the past two years, growth within the CWID community necessitated network architecture modifications to support the ever changing CWID environment. Following several years operating on the established Combined Federated Battle Laboratories Network (CFBLNet), CWID 2005 designed a new, scalable and flexible network that incorporated both a change in physical architecture as well as a change in how participating nations were viewed. This network, known as the Purple Enclave, was built separately from the traditional CFBLNet and was successfully implemented to support CWID 2005.

CWID 2006 faced new challenges that led to development of the Coalition Task Force/ NATO Response Force (CTF/NRF) Enclave.

CWID 2006 faced new challenges that led to the development of the Coalition Task Force/NATO Response Force CTF/NRF (CTF/NRF) Enclave, an additional network that provides increased scalability and flexibility over the Purple Enclave. To accommodate U.S. Northern Command's (USNORTHCOM) interests toward Homeland Security, CWID also built an unclassified network, the Homeland Security/Homeland Defense (HLS/HLD) Enclave.

THE CTF/NRF ENCLAVE

The CTF/NRF Enclave utilized the CFBLNet backbone Asynchronous Transfer Mode (ATM) transport layer which tunneled through the Defense Information Systems Network-Leading Edge Services (DISN-LES) Public ATM (PATM) infrastructure and the DISA ATM Services - Unclassified



(DATMS-U) ATM backbone networks. Designed as a secret-releasable overlay on the CFBLNet backbone ATM and Internet Protocol (IP) transport, the CTF/NRF Enclave incorporated a combination of classified ATM and IP backbone, capable of supporting high-speed data transmission requirements of up to 45 Mega bytes per second (Mbps). In the U.S., the CTF/NRF shared between 3 and up to 40 Mbps of bandwidth on the DISN-LES with the HLS/HLD enclave depending on needs and locations of individual sites.

The CTF/NRF Enclave consisted of nine U.S. and five Coalition sites. The network concept was built on a basic security enclave, isolated from the DISN-LES by type 1 encryption, and only containing data classified secret-releasable to all participating nations.

Throughout the demonstration, the CTF/NRF Enclave availability was 99.99 percent based on IP connectivity during the CWID day.

THE HLS/HLD ENCLAVE

The HLS/HLD network underwent a significant redesign, establishing a completely new architecture for CWID 2006. Built as a subset of the existing DISN-LES network architecture, it utilized both existing services and those established solely for CWID 2006. Each HLS/HLD site received or provided a Cisco router and switch to support the demonstration and a PacketShaper to monitor site network traffic as well as provide reports. In addition, a new private IP addressing scheme was established and used throughout the event. This year marked the first time Canada and U.S. European Command (USEUCOM) joined the HLS/HLD Enclave and fully participated with USNORTHCOM testing and evaluating HLS/HLD technologies.

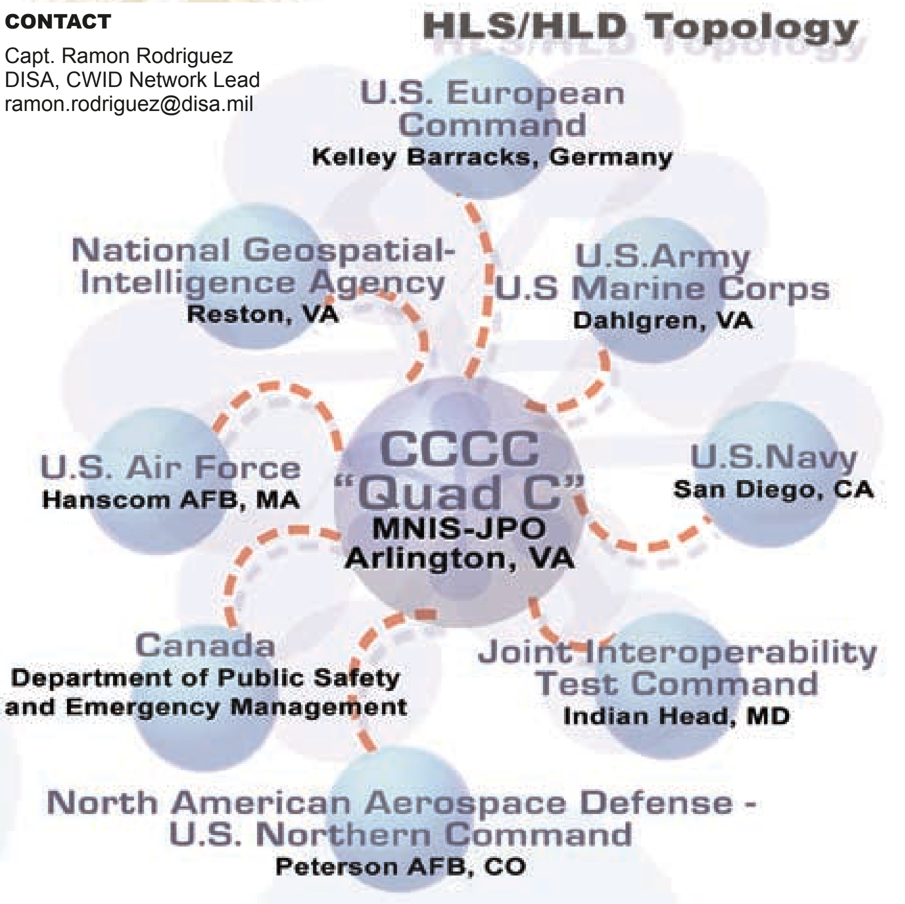
One of the most important changes for CWID 2006 was a direct public Internet connection for the HLS/HLD network. A 3Mbps connection was provided by a local Internet Service Provider (ISP) and terminated at the Multinational Information Sharing Joint Program Office (MNIS-JPO) (known as CCCC, or "Quad C" for Combined Command and Control Center). During previous years, all firewall/ports/protocols change requests required clearance by Non-secure Internet Protocol Router Network (NIPRNet) authorities, a tedious and time consuming process. By removing the NIPRNet as the Internet source, the CCCC controlled all ports and protocols for Internet connection, allowing greater flexibility to accommodate trials' requests and troubleshooting connectivity issues. These approaches also allowed for a less restrictive, yet secure, Internet connection, and allowed trials to successfully complete a larger number of scenario events.

Another critical change for CWID 2006 was using Virtual Private Networks (VPNs) to set up secure connections from remote agents/trials/organizations to the HLS/HLD network via the Internet. CCCC engineers successfully established VPN connectivity between two agency LANs and the HLS/HLD network, U.S. National Guard and the U.S. California Customs. In addition, a field police cruiser successfully established a VPN from his laptop computer into the HLS/HLD network. CCCC Engineers successfully monitored the network 24/7 from remote locations via a VPN connection into the HLS/HLD management LAN.

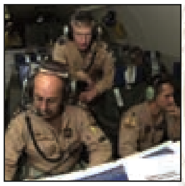
Throughout the demonstration, the HLS/HLD Enclave availability was 100 percent based on IP connectivity during the CWID day.

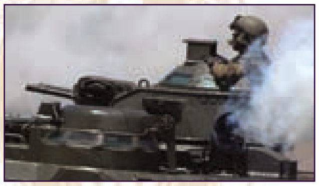
CONTACT

Capt. Ramon Rodriguez
DISA, CWID Network Lead
ramon.rodriguez@disa.mil



> *This year marked the first time Canada and USEUCOM joined the HLS/HLD Enclave and fully participated with USNORTHCOM testing and evaluating technologies.*





A MULTINATIONAL PERSPECTIVE

NATO Leverages CWID Forum

The cornerstone of NATO's transformational capability is the NATO Response Force (NRF). By design, forces will be agile, joint and expeditionary and must be supported by "network-enabled capabilities based on a robust and flexible Computer Information Systems (CIS) foundation."

The shared vision of the two Strategic Commands (Allied Command Operations and Allied Command Transformation) is that NATO forces, including the NRF, achieve Decision Superiority that in turn is enabled by achieving Information Superiority through networked forces. Allied Command Transformation (ACT) is therefore engaged in efforts to create forces that are capable of achieving this type of Decision Superiority.

ACT drives development of concepts and systems that can achieve Information Superiority. These concepts and systems are tested and validated using the full spectrum of available exercises, trials, and experiments – such as CWID.

NATO CWID 2006

NATO used CWID 2006 to progress Transformation within the Alliance. ACT aligned aspects of the Scientific Programme of Work (SPOW) activities with NATO CWID testing activities. As a result, capabilities were examined to support the rollout of NATO Network Enabled Capability (NNEC) through testing and evaluation. As proposed by the NATO Headquarters Command, Control and Communications (C3) staff, NATO CWID was used as a test venue to validate interoperability of NATO and national Command, Control and Information Systems (C2IS) planned or projected to be committed to NRF Rotation 5 (NRFs 9 and 10). Operational commitments commence in July 2007. Interoperability issues that were identified as a result of trials conducted in NATO CWID can be addressed and resolved prior to that time.

2006 NATO CWID OBJECTIVES

In addition to the five CWID Objectives, there were two specific NATO objectives for 2006:

OBJECTIVE 1:
■ Conduct testing to validate the interoperability between C2IS required in NRF rotations 9 and 10 in support of the certification process.

OBJECTIVE 2:
■ Provide network tools to facilitate the management of information, enabling automatic discovery and integration technologies that promote loose coupling between Command and Control (C2) systems and components.

NATO CWID EXECUTION SITE

Camp Jorstadmoen in Lillehammer, Norway hosted the NATO 2006 CWID event. The Camp has a military history dating back to 1750 and has been in use by the Norwegian Army Signal Corps since 1945. The Camp was selected by the Norwegian parliament to be the site of the Joint CIS Training Centre within Norway and has taken on this new role, which compliments the Joint and Coalition nature of the testing conducted in NATO CWID 2006.

POINTS OF CONTACT

Cmdr. Clark Price
NATO CWID Director
ACT/C4I
cprice@act.nato.int
+1 757 445 3556

Mr. D.C. Taylor
NATO CWID Senior Analyst
ACT/C4I
dtaylor@act.nato.int
+1 757 445 3556

GO TO CD HOME PAGE

NETWORK TOPOLOGY, NATO DOMAIN, LILLEHAMMER

The NATO CWID 2006 network at Camp Jorstadmoen was built around a common domain referred to as the Coalition Task Force (CTF)/NRF domain. This domain was referred to as the NATO CWID 'purple' domain.

Several nations used Information Exchange Gateways (IEGs) to separate their national Local Area Networks (LANs) from the common domain, thereby analyzing the interoperability over their cross-domain solutions.

While the NATO CWID network architecture's primary was Camp Jorstadmoen, there were additional national sites where NATO CWID tests were conducted.

ACT drives the development of concepts and systems that can achieve Information Superiority. These concepts and systems are tested and validated using ...available exercises, trials, and experiments – such as CWID.

PARTICIPATING NATIONS AND AGENCIES

There were 19 nations and agencies actively participating from the NATO execution site in Lillehammer and an additional 3 nations who attended as observers. NATO C2 systems from each of the operational environments (Maritime Command and Control Information Systems [MCCIS], air Integrated Command and Control [ICC] and Land Command and Control Information Systems [LCCIS]) were tested.

THE NATO SCENARIO AND NRF STRUCTURE

The NATO Scenario was designed for the NATO Response Force, which is driven by the underlying principles: "first force in, first force out" and tailored for a specific mission. The NATO scenario complemented the US scenario. Within this scenario, the NRF could perform certain missions on its own, as well as participating with the U.S. CTF. Deployed as a stand-alone force for Crisis Response, the NRF scenario had the following capabilities:

■ Evacuate non combatants from a crisis area

■ Support consequence management (including chemical, biological, radiological and nuclear incidents)

■ Support in a humanitarian crisis situation

■ Manage crisis response operations, including peacekeeping

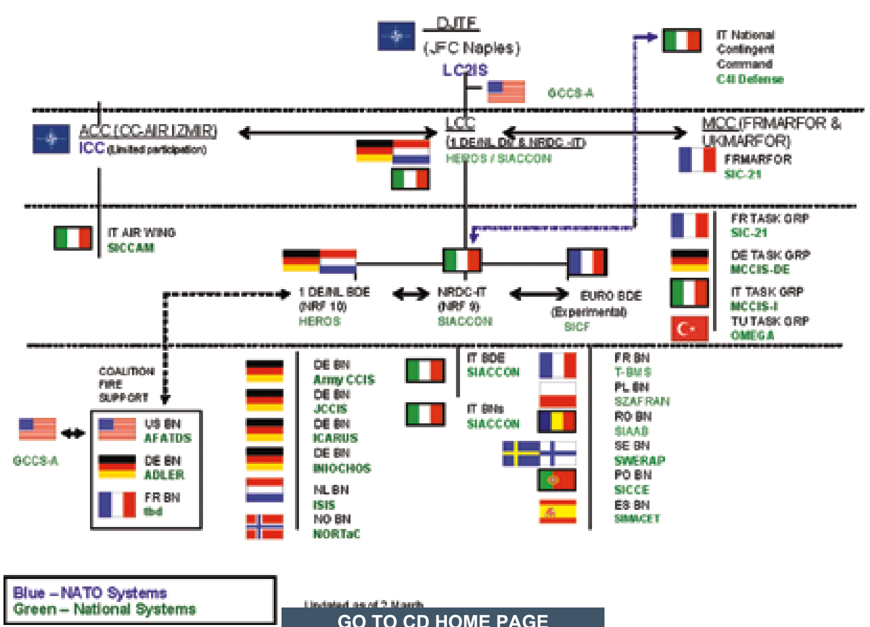
■ Counter terrorism operations

■ Embargo operations

The NATO CWID Scenario flexibility gave it unique character, enabling tailoring to test interoperability of NATO and national C2 systems as well as individual Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) trials. Scenario Command and Control structure and related NATO and national C2 systems and interactions that were used for NATO CWID 2006 is depicted in the diagram, lower center of this page.

For 2006 the NRF structure was loosely based on NRF rotations nine and ten. It operated under the command and control of a Joint Force Headquarters that extracted a permanent Deployable Joint Task Force staff as a forward command element. The NRF Air component provided a capability to conduct appropriate air tasks. NRF Land Components contained a structure sufficient to allow deployment of a tailored brigade size formation composed of manoeuvre elements and the requisite support and breadth of assets to allow it to conduct a wide range of land tasks. The NRF Maritime components comprised a force up to a NATO task force size including a carrier battle group with associated surface and subsurface combat units, amphibious forces, naval Mine Countermeasures (MCM) units and auxiliary support vessels.

Scenario C2 Structure & Core NRF-related System Interactions



NOTES

TRIALS SUMMARY CONTENTS PAGE

Interoperability Trials

CWID trials for 2006 are listed in trial number order below, cross referenced to sites where they were assessed during the demonstration 12 to 22 June.

OBJECTIVES KEY

1. COALITION C2 ■
2. COALITION INFORMATION SHARING ■
3. INTEGRATED LOGISTICS ■
4. CONTINUITY OF OPERATIONS ■
5. NET-CENTRIC ENTERPRISE SERVICES ■

TRIAL NO.	SYSTEM TITLE	USEUCOM	USNORTHCOM	NSWC DAHLGREN	SPAWAR	HANSCOM	AUSTRALIA	CANADA	NEW ZEALAND	UNITED KINGDOM	NATO	GOVERNMENT SPONSOR	GOVERNMENT/ CORPORATE DEVELOPER/S	OBJECTIVE/S ADDRESSED	PAGE NO.
IT01.01	Northern European Command - C2 Information System (NEC CCIS)					■				■		Denmark	NATO, Denmark	**5**, 1, 4	**15**
IT01.14	U.S. Chemical Biological Radiological and Nuclear Modeling (USCBRNM)			■						■		Joint Project Manager Information Systems (JPM IS); UK Defense Science & Technology Laboratories (Dstl), International Task Force 49	JPM IS, Dstl International Task Force 49	**1**	**15**
IT01.15	C4I Defense	■		■	■	■					■	Italy	C3I Consortium, SELEX-SI SpA	**1**, 4	**16**
IT01.20	Integrated Information Management System			■	■		■					US Air Force	US Army, AFRL	**1**, 5	**16**
IT01.28	Mission Management Suite (MMS)					■	■	■	■			Canada	Canadian Air Force, ATESS Trenton	**1**	**17**
IT01.34	Mobile/Static Real-Time Radiological Surveillance Network (MobRadNet)		■		■			■				Canada	Dr. Robert McFadden	**1**	**17**
IT01.39	FIRST Responder INTERoperable COMMunications (First InterComm™)		■									USNORTHCOM	BAE Systems	**1**	**18**
IT01.48	Coalition Incident Response-Common Operating Picture (CIR-COP)		■	■								National Guard Bureau	National Guard Bureau	**1**	**18**
IT01.50	Multinational Interoperability Toolkit (MIT)	■			■		■					US Navy	SPAWAR	**1**	**19**
IT01.53	Coalition and Civil Agency Capable Wireless Information Transfer System (C3WITS)	■	■	■	■							US Navy	General Dynamics C4 Systems	**1**, 5	**19**
IT01.54	Coast Guard C2 (Deepwater COP) (CG-C2)		■	■	■							US Coast Guard	Lockheed Martin Corporation	**1**	**20**
IT01.62	MobileForcesSolution (MOFS / MCCIS)				■						■	Germany	German Navy, T-Systems Enterprise Services GmbH	**1**, 4, 5	**20**

Continued next page

TRIAL SUMMARY

OBJECTIVES KEY
1. COALITION C2 ■
2. COALITION INFORMATION SHARING ■
3. INTEGRATED LOGISTICS ■
4. CONTINUITY OF OPERATIONS ■
5. NET-CENTRIC ENTERPRISE SERVICES ■

TRIAL NO.	SYSTEM TITLE	USEUCOM	USNORTHCOM	NSWC DAHLGREN	SPAWAR	HANSCOM	AUSTRALIA	CANADA	NEW ZEALAND	UNITED KINGDOM	NATO	GOVERNMENT SPONSOR	GOVERNMENT/ CORPORATE DEVELOPER/S	OBJECTIVE/S ADDRESSED	PAGE NO.
IT01.63	IPC Information Systems, LLC Multimedia Command and Control Solution (MCCS)		■	■								FEMA	IPC Command Systems	**1**	21
IT02.21	The Multi National Coalition Security System (MNCSS)			■	■	■	■	■	■	■		Canada	Titus Labs, Microsoft Corp.	**2**, 5	21
IT02.24	M3Data Information Sharing System (M3Data ISS)							■		■		Canada	ARTIS	**1**, 5	22
IT02.25	Distributed Common Ground System (DCGS)			■	■	■		■		■		Canada	Raytheon Intelligence and Information Systems	**2**	22
IT02.45	Command Center Portal Framework (CCPF)		■				■	■	■	■		Canada	xwave	**2**	23
IT03.09	Document Access Servelet (DAS)		■	■	■	■		■	■			USEUCOM	Information Security Corpo-ration	**5**	23
IT03.16	Intelligent Road/Rail Information Server (IRRIS)	■	■	■	■							US Army	US Army, GeoDecisions	**3**, 5	24
IT04.03	Wide Area Interoperability System (WAIS) and ACU-1000		■									USNORTHCOM	Raytheon JPS Communica-tions	**1**, 5	24
IT04.33	Logik v3.0 for Rapid Intelligence Analysis and Exploitation	■	■	■	■			■		■		Canada	Coredge Soft-ware, iFathom Corpo-ration	**4**	25
IT04.36	Global Broadcast Service (GBS)		■	■								DISA	GBS JPO	**1**, 4, 5	25
IT04.46	Joint C4 Coordination Support System (JCCSS)		■	■								National Guard Bureau	National Guard Bureau	**4**	26
IT04.61	Maritime Command and Control Information System - Italy				■						■	Italy	Italy, Canada, NATO ACT, Engineering SpA Rome	**1**	26
IT05.06	Visualization for Information Assurance (VIA)			■					■			US Air Force	Applied Visions, Inc.	**5**, 1, 2	27
IT05.13	Coalition Command Collaboration Services (CCCS)						■	■	■			Australia	Microsoft Corp.	**4**, 1	27
IT05.17	WMD Collaborative Advisory Response System (WMDCARS)	■	■				■					DTRA	DTRA	**5**	28
IT05.32	Guard Net Portal (GNP)	■	■	■	■							US Navy	Tidewater Technology Group	**1**, 5	28
IT05.37	Joint Effects Based Command and Control (JEBC2)	■	■		■			■				USNORTHCOM	The Boeing Company	**1**, 2, 3, 5	29
IT05.41	Knowledge Management Framework							■				Canada	Lockheed Mar-tin Corporation	**5**	29
IT05.47	HLS/HLD Collaborative Informa-tion Exchange Environment (HLS/HLD CIEE)		■	■								National Guard Bureau	National Guard Bureau	**5**	30
IT05.51	FORCEnet Distributed Channel Services (FnDCS)	■		■	■		■		■	■		US Navy	Lockheed Mar-tin Corporation	**5**, 1	30
IT05.52	Rapid Triage Medical Workbench (RTMW)		■	■	■			■				USNORTHCOM	AMITA Corporation	**5**, 3	31
IT05.66	Coalition Shared Information Environment (COSINE)	■					■					NATO	NATO NC3A	**2**, 5	31
HISTORY															32

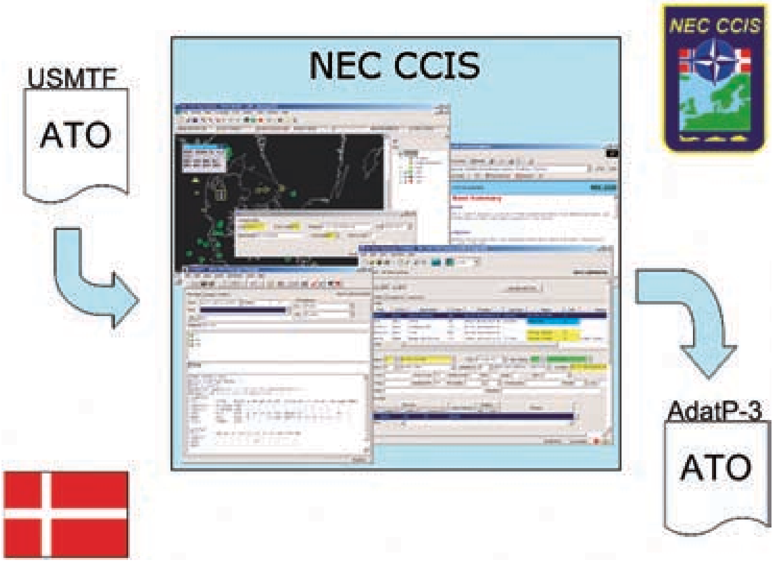
GO TO CD HOME PAGE

IT01.01
Northern European Command C2 Information System

1. COALITION C2 ● 4. CONTINUITY OF OPERATIONS ● 5. NET-CENTRIC ENTERPRISE SERVICES ●

TRIAL OVERVIEW: Northern European Command C2 Information System (NEC CCIS) is a tri-service C2IS sponsored by NATO, Denmark and Norway and used for air operations planning and tasking within the Royal Danish Air Force and Royal Norwegian Air Force. NEC CCIS has a three-tier architecture with an Oracle database, an application server and an XML-based client. NEC CCIS, a fielded NATO Air C2 system, offers a number of interfaces such as USMTF, ADatP-3, OTH-GOLD, Link 1, and ICC. It can map dedicated messages into the database (e.g. ATO). NEC CCIS forms the foundation for the planning/tasking of NATO Air Command and Control Systems and is usable from headquarters level through Coalition Air Operations Center (CAOC) to Control and Reporting Centers (CRCs), wing and squadron levels.

SPONSOR: Denmark
TRIAL LOCATIONS:
Hanscom AFB, UK
TRIAL PARTNERS: None



WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING
GO TO CD TRIAL DIRECTORY
GO TO CD HOME PAGE

ASSESSMEMT RESULTS:
During CWID 2006, NEC CCIS received a SEIWG evaluation report.

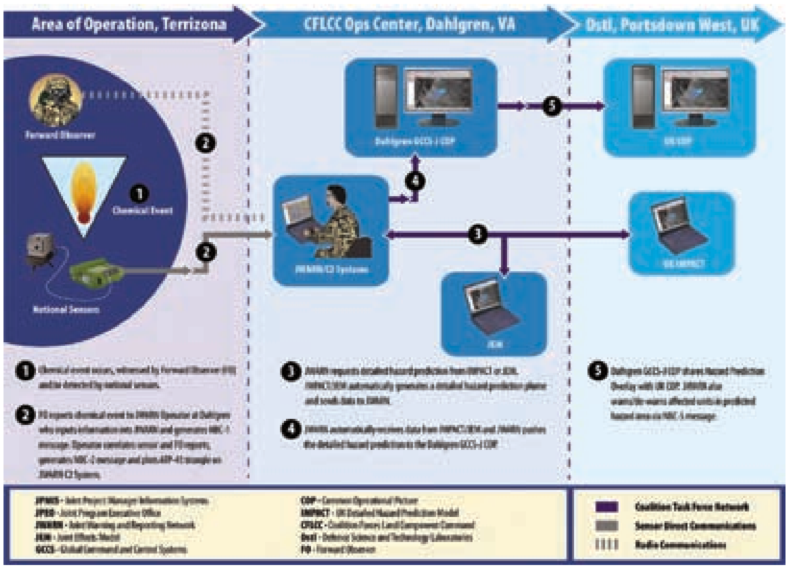
- NEC CCIS successfully met CWID Objectives 1, 4 and 5.
- NEC CCIS translated ACO and ATO USMTF messages from TBMCS, a US system, to ADatP3-B11 message formats used by NATO systems.
- Successfully forwarded and shared information in a multi-national environment with coalition C2 systems providing horizontal and vertical information dissemination by posting a translated ATO/ACO text file the NEC CCIS portal.

IT01.14
U.S. Chemical, Biological, Radiological and Nuclear Modeling

1. COALITION C2 ●

TRIAL OVERVIEW: The U.S. Chemical, Biological, Radiological and Nuclear Modeling (USCBRNM) System trial was designed to demonstrate interoperability and information sharing between two U.S. systems, Joint Effects Model (JEM) and Joint Warning and Reporting Network (JWARN), and two U.K. systems, U.K. IMPACT detailed hazard prediction model and U.K. SAFE prototypical warning and reporting network. USCBRNM provides improved interoperability of U.S., U.K. and Canadian chemical, biological, and radiological (CBR) warning, reporting and modeling capabilities within a multinational, coalition environment. JEM and the IMPACT CBRN modeling system are an enterprise service for CWID. JWARN requests hazard prediction from JEM and IMPACT, displaying predicted hazards to decision makers.

SPONSORS: Joint Project Manager Information Systems (JPM IS); UK Defense Science & Technology Laboratories (dstl)
TRIAL LOCATIONS:
NSWC Dahlgren, UK
TRIAL PARTNERS: None



1 Chemical event occurs, witnessed by Forward Observer (FO) and be detected by national sensors.

2 FO reports chemical event to JWARN Operator at Dahlgren who inputs information into JWARN and generates NBC-1 message. Operator correlates sensor and FO reports, generates NBC-2 message and plots ATP-45 triangle on JWARN C2 System.

3 JWARN requests detailed hazard prediction from IMPACT or JEM. IMPACT/JEM automatically generates a detailed hazard prediction plume and sends data to JWARN.

4 JWARN automatically receives data from IMPACT/JEM and JWARN pushes the detailed hazard prediction to the Dahlgren GCCS-J COP.

5 Dahlgren GCCS-J COP shares Hazard Prediction Overlay with UK COP. JWARN also warns/re-warns affected units in predicted hazard area via NBC-3 message.

JPMIS - Joint Project Manager Information Systems
JPEO - Joint Program Executive Office
JWARN - Joint Warning and Reporting Network
JEM - Joint Effects Model
GCCS - Global Command and Control Systems
COP - Common Operational Picture
IMPACT - UK Detailed Hazard Prediction Model
CFLCC - Coalition Forces Land Component Command
Dstl - Defence Science and Technology Laboratories
FO - Forward Observer

■	Coalition Task Force Network
■	Sensor Direct Communications
‖‖	Radio Communications

WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING

ASSESSMEMT RESULTS:
During CWID 2006, the US-CBRNM System received a SEIWG evaluation report.

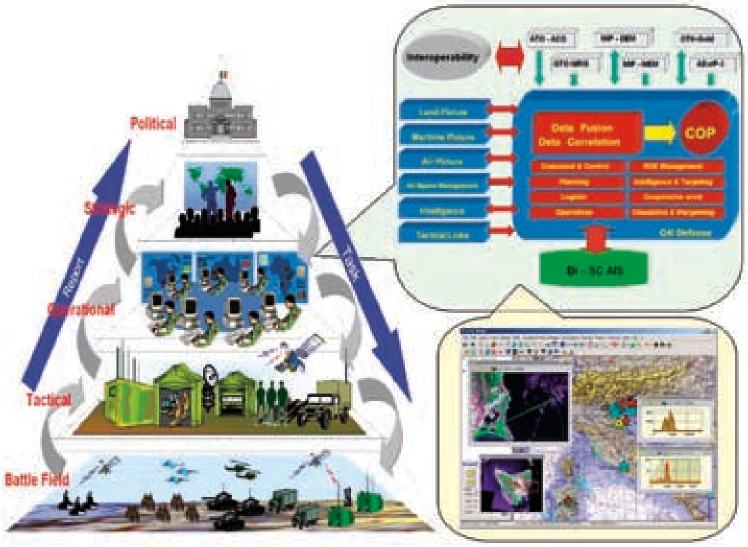
- USCBRNM successfully demonstrated CWID Objective 1 by creating interfaces between U.S. and U.K. CBR systems supporting continued coalition CBR interoperability.
- USCBRNM established new plume generation requirements for the JEM urban dispersion model based on the enhanced capabilities demonstrated by the IMPACT CBR system.
- Successfully established coalition CBR working relationships supporting the evolution of CBR data models and CBR interoperability standards.

IT01.15
C4I Defence

1. COALITION C2 ● 4. CONTINUITY OF OPERATIONS ●

TRIAL OVERVIEW: C4I Defence demonstrates interoperability among Command and Control (C2) systems of Italian Armed Forces (Army, Navy, and Air Force) and the Italian Command and Control Joint System (C4I Defense) or among allied C2 systems and the Italian C4I Defense System. C4I Defence provides top-level strategic capabilities, above the tactical functionalities offered by the Command and Control systems of each Armed Force. It supports the Operational Commander in Operations Planning and Tasking (Orders Generation) and in Tactical Situation Analysis and Monitoring. C4I Defense exchanges both TOP COP data and single component picture (RMP, RAP, RGP) and can operate either as a top-level strategic system or as a tactical system.

SPONSOR: Italy
TRIAL LOCATIONS:
USEUCOM, NSWC Dahlgren,
SPAWAR, Hanscom AFB,
NATO
TRIAL PARTNERS: None



WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING
GO TO CD TRIAL DIRECTORY
GO TO CD HOME PAGE

ASSESSMEMT RESULTS:
During CWID 2006, the C4I Defence Trial received a Technical Interoperability assessment.

■ During CWID 2006 the Italian C4I Defence System successfully tested technical interoperability between U.S. and Italian command and control systems, satisfying CWID Objective 1.

■ C4I Defence, interoperated with GCCS-J and GCCS–M, exchanging messages in various standard formats e.g. OTH-Gold messages and ATO/ACO messages in MTF format between SPAWAR, USEUCOM, and Lillehammer, Norway.

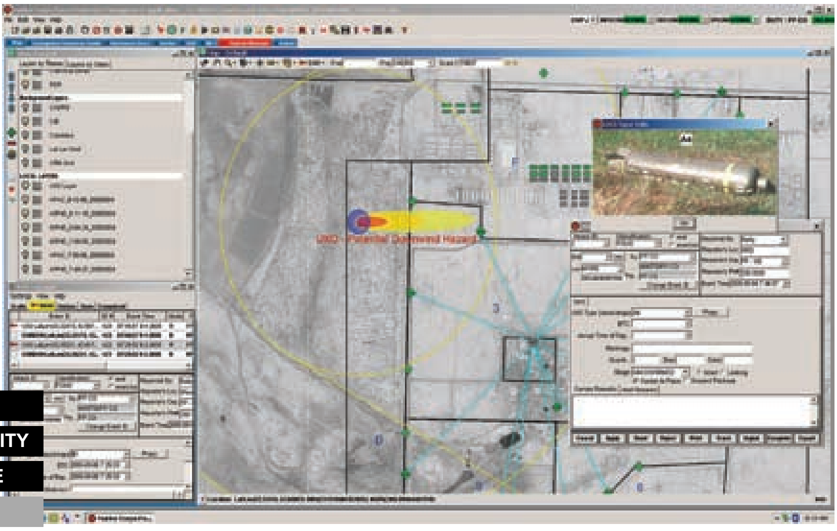
■ C4I Defence provided continuity of operations (CWID Objective 4) by supplying unit/track data, enhancing the Commander's situational awareness and ability to plan, communicate and affect coalition operations while remotely deployed.

IT01.20
Integrated Information Management System

1. COALITION C2 ● 5. NET-CENTRIC ENTERPRISE SERVICES ●

TRIAL OVERVIEW: The Integrated Information Management System (IIMS) is a collaborative situation awareness tool. IIMS aids fixed, expeditionary and incident response sites plan, protect against, and recover from chemical, biological, radiological, nuclear (CBRNE) or conventional attacks. It decreases the time needed for site operations to recover from attacks using rapid manual data entry, data transfer across air gap or guard onto a Common Operational Picture (COP) for the Commander and geographically separated Unit Control Centers. Earlier versions of IIMS are fielded at PACAF and USCENTCOM. For CWID 06 IIMS focused on selective information sharing across domains using techniques from manual entry to sending through a one-way guard to support Coalition Command and Control, and Net Centric Enterprise.

SPONSOR: US Air Force
TRIAL LOCATIONS:
NSWC Dahlgren,
SPAWAR, Australia
TRIAL PARTNERS: IT05.37



WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING

ASSESSMEMT RESULTS:
During CWID 2006, IIMS received Warfighter, Technical Interoperability and Information Assurance assessments.

■ IIMS successfully met CWID Objectives 1 and 5. IIMS enabled sharing CBRNE information in electronic attack reports (EARs) and USMTF/ADatP-3 message formats within and/or across domains by moving via a data diode, transferring via CD, or manually inputting the information. IIMS delivered track data to the JWARN/GCCS system using the Common Message Protocol (CMP).

■ IIMS experienced network difficulties, and at times, could not claim enough bandwidth to permit information sharing between the server and client.

■ Information Assurance (IA) scans identified open ports with no associations which should be closed to prevent security breaches.

■ IA testing also found 16 High, 3 Medium, and 9 low vulnerabilities to include deficient Oracle patch incorporation and other faults such as Web Log Analyzer, ICMP Time Requests, FTP, TELNET, and other open services.

GO TO CD HOME PAGE

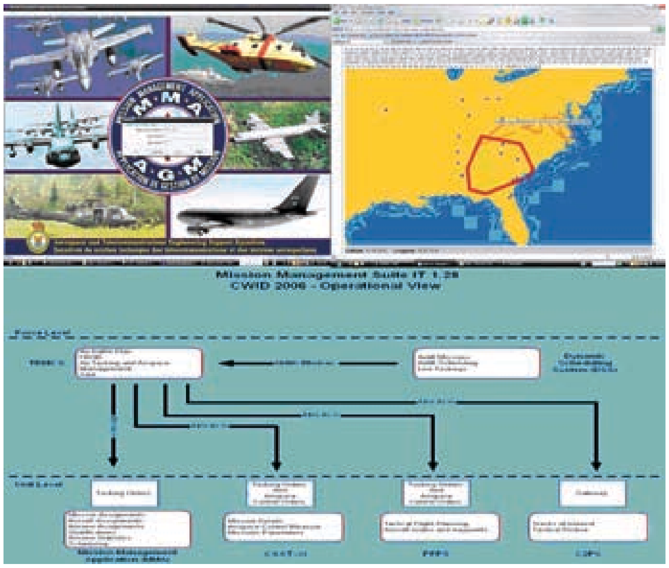
IT01.28

Mission Management Suite

1. COALITION C2 ●

TRIAL OVERVIEW: The Mission Management Suite (MMS) is an integrated flexible suite of mission planning tools for managing Air Force Missions from Force to Unit Level at home base or deployed locations. It provides the ability to parse mission details and assign resources to support tasks. The suite also offers functions such as aircraft and aircrew scheduling, flight planning, aircraft and aircrew management and cost centre management. In an environment where unit-level mission management tools are either limited or non-existent, MMS is the first spiral toward Unit Level automation.

SPONSOR: Canada
TRIAL LOCATIONS:
Canada,
Hanscom AFB,
Australia, New Zealand
TRIAL PARTNERS: None


M·M·A
A·G·M
Mission Management Suite IT 1.28
CWID 2006 - Operational View

WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING
GO TO CD TRIAL DIRECTORY
GO TO CD HOME PAGE

ASSESSMEMT RESULTS:
During CWID 2006, the MMS Trial received Warfighter and Technical Interoperability assessments.

■ MMS provided a suite of tools that enhanced the commanders' coalition command and control capability and allowed users to visualize mission data, manage aircrew and fleet schedules as well as capture and track the required resources.

■ MMS successfully demonstrated Joint Command and Control by parsing and manipulating ATO/ACOs in text and XML format and exchanging data with the U.S. TBMCS.

■ Warfighters generally agreed the tool suite was well integrated and intuitive but noted some overlap in functionalities. However, the Mission Management Application was not as user-friendly for some warfighters.

■ Lack of on-site training and on-site technical support kept some warfighters from taking advantage of the systems' full functionality.

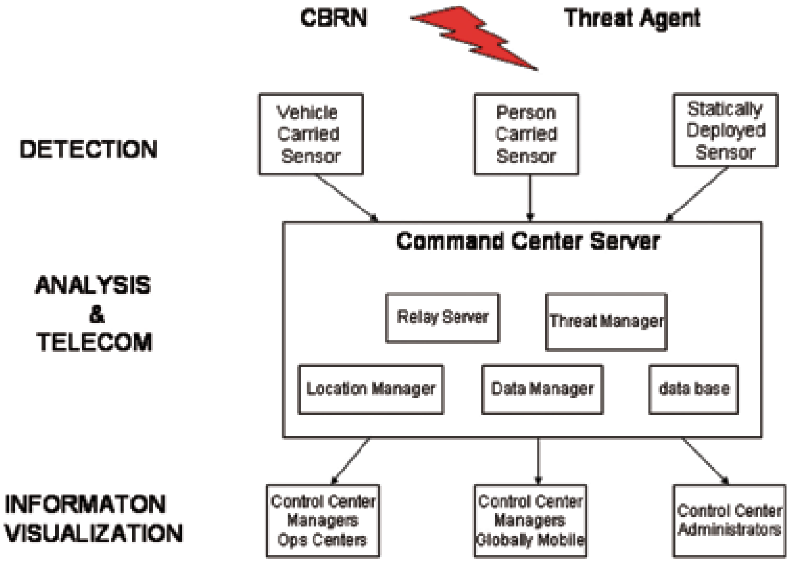
IT01.34

Mobile/Static Real-Time Radiological Surveillance Network

1. COALITION C2 ●

TRIAL OVERVIEW: The Mobile/Static Real-Time Radiological Surveillance Network (MobRadNet) is a real-time radiation surveillance system using mobile and/or fixed detectors. The system instantly alerts military and civilian authorities of radioactive materials during any radiological event. MobRadNet is easily deployable, uses existing technologies and incorporates an integratable, scalable network interface and Geographic Information System. It provides a real-time understanding of the task force operating area radiological environment and enables specific radiological context common view sharing. The autonomous operation of a rapidly deployable/re-deployable network of gamma sensors provides consistent and reliable radiological data from unattended operations whether mobile (vehicle or person carried) or static.

SPONSOR: Canada
TRIAL LOCATIONS: Canada, USNORTHCOM, SPAWAR
TRIAL PARTNERS: None



WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING

ASSESSMEMT RESULTS:
During CWID 2006, the MobRadNet Trial received Warfighter, Technical Interoperability and Information Assurance assessments.

■ MobRadNet successfully enhanced the commander's coalition command and control capability by providing real-time access to radiological measurement data through a mapping interface.

■ Provided real-time radiological data collected by sensors at various locations and transmitted data via a cellular data network to a centralized server. Users received data as meaningful graphic representations over the network.

■ A detractor to the trial was that Trojan signatures were found on several open ports as well as a vulnerability that could allow attackers to gain access via a remote host.

■ MobRadNet successfully demonstrated a network-based radiological surveillance system allowing for streamlined decision-making supporting Global War on Terrorism (GWOT) contingencies.

IT01.39

FIRST Responder INTERoperable COMMunications

1. COALITION C2 ●

TRIAL OVERVIEW: First InterComm allows first responders with dissimilar radios to communicate with each other using the radio frequency of that First Responder Agency. The shoebox-sized unit mounted inside first responder vehicles links all vehicles at an incident scene, operates on the vehicle's battery, and automatically creates temporary networks for interoperability with civil and military radios, requiring no operator involvement. First InterComm provides a digital solution compatible with the latest (P-25) radios, does not require a tower for local interoperability, and eliminates the need for additional radios for cross-jurisdictional support. Combining First InterComm's advanced technology, developed for the military, with commercial off-the-shelf software, the system provides a mature, reliable and cost-effective wireless interoperability capability.

SPONSOR: USNORTHCOM
TRIAL LOCATIONS:
USNORTHCOM
TRIAL PARTNERS: None

010101010101010101010
0101010101010101010

WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING
GO TO CD TRIAL DIRECTORY
GO TO CD HOME PAGE

ASSESSMEMT RESULTS: During CWID 2006, the FIRST-InterComm Trial received Warfighter and Technical Interoperability assessments.

■ First InterComm successfully met CWID Objective 1 by providing interoperability voice communications to First Responders creating a cohesive relationship between military and civilian agencies.

■ Successfully demonstrated bridging dissimilar radios on different frequencies establishing a remote mesh network at the incident scene supporting Homeland Security/Homeland Defense.

■ First InterComm was easy to use and required minimal training.

■ The Incident Commander established separate talk groups, while monitoring and maintaining all communications and operational control at the scene.

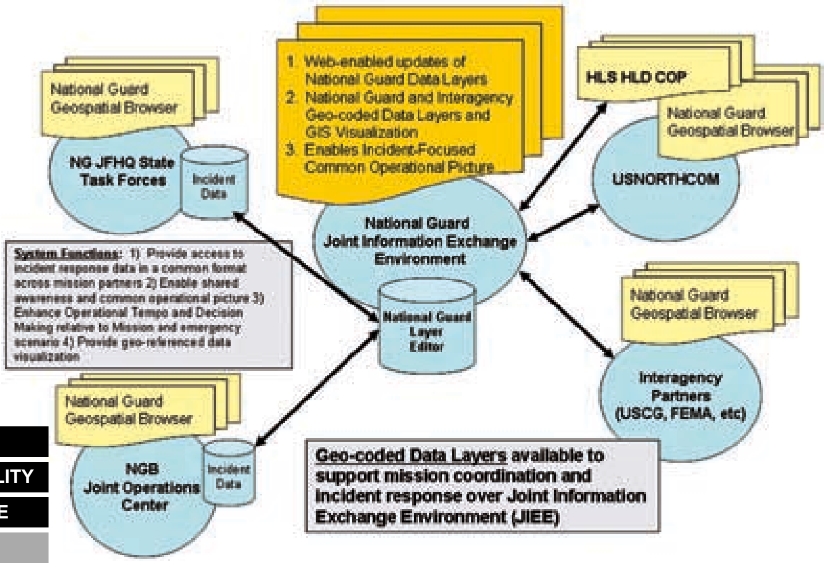
IT01.48

Coalition Incident Response - Common Operating Picture

1. COALITION C2 ●

TRIAL OVERVIEW: Coalition Incident Response–Common Operation Picture (CIR-COP), a National Guard Bureau initiative, supports coordination of regional incident responses, and provides National Guard-focused information supporting critical C2 decisions at all operational levels and critical C2 decision points. CIR-COP provides access to incident response data in a common formation, improves shared situational awareness, provides geo-referenced data visualization, and provides National Guard mission partners the ability to view and update COP data layers through web-enabled forms.

SPONSOR: National Guard Bureau
TRIAL LOCATIONS:
USNORTHCOM,
NSWC Dahlgren
TRIAL PARTNERS:
IT04.46, IT05.47


National Guard Geospatial Browser
NG JFHQ State Task Forces
Incident Data
1. Web-enabled updates of National Guard Data Layers
2. National Guard and Interagency Geo-coded Data Layers and GIS Visualization
3. Enables Incident-Focused Common Operational Picture
HLS HLD COP
National Guard Geospatial Browser
USNORTHCOM
National Guard Joint Information Exchange Environment
National Guard Layer Editor
National Guard Geospatial Browser
Interagency Partners (USCG, FEMA, etc)
National Guard Geospatial Browser
NGB Joint Operations Center
Incident Data

System Functions: 1) Provide access to incident response data in a common format across mission partners 2) Enable shared awareness and common operational picture 3) Enhance Operational Tempo and Decision Making relative to Mission and emergency scenario 4) Provide geo-referenced data visualization

Geo-coded Data Layers available to support mission coordination and incident response over Joint Information Exchange Environment (JIEE)

WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING

ASSESSMEMT RESULTS: During CWID 2006, the CIR-COP Trial received Warfighter and Technical Interoperability assessments.

■ CIR-COP built a National Guard COP to support C2 and coordinate decision-making and operations across mission space by sharing GIS XML Data Layers, successfully demonstrating Objective 1.

■ CIR-COP provided access to incident site, state, regional critical information required to support decision-making, force structuring, and capabilities around each operational phase organized by C2 (e.g. Joint C4 Response, Logistics, Medical, Force etc.).

■ CIR-COP provided a common data format to share information with the overall HLS/HLD Common Operational Picture and mission partners.

GO TO CD HOME PAGE

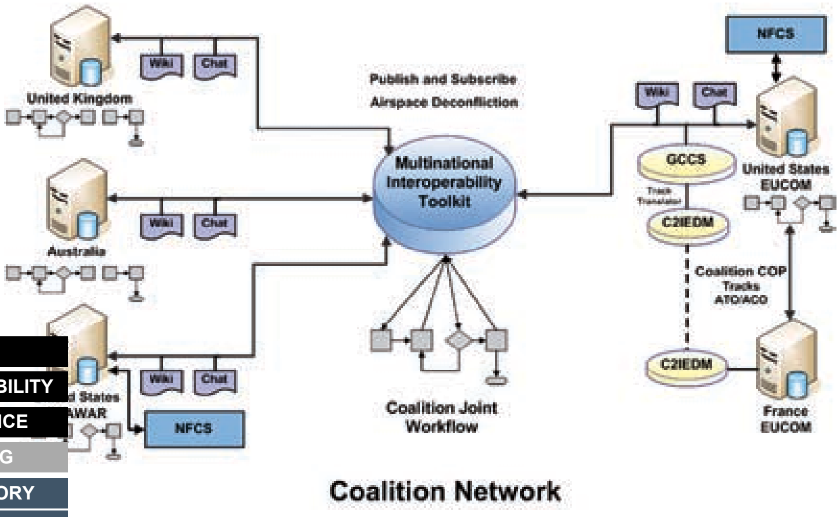
IT01.50

Multinational Interoperability Toolkit

1. COALITION C2 ●

TRIAL OVERVIEW: The Multinational Interoperability Toolkit (MIT) provides capabilities that enhance coalition interoperability and automate Common Operational Picture (COP) interoperability in a tactical environment using multiple standards. The toolkit combines the strengths of formal messaging and informal collaboration to create a workflow-enabled coalition enterprise. MIT components provide Publish, Subscribe and Web services infrastructure supporting COP and other C2 data exchange, a translation layer to and from the Multinational Interoperability Program Command and Control Information Exchange Data Model (C2IEDM) data model, and interoperability between XML, C2IEDM and the family of Global Command and Control systems (GCCS) based on DISA Common Operating Environment Version 4.

SPONSOR: US Navy
TRIAL LOCATIONS: USEUCOM, SPAWAR, Australia
TRIAL PARTNERS: None



WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING

GO TO CD TRIAL DIRECTORY
GO TO CD HOME PAGE

ASSESSMEMT RESULTS:
During CWID 2006, the MIT Trial received Warfighter and Technical Interoperability assessments

■ MIT marginally satisfied CWID Objective 1 because MIT internal features and external interfaces (the SPARK Chat tool, WIKI dynamic web pages, and JASMAD) required repeated resetting/or refreshing to operate properly. The reset/refresh delays were a detriment to providing timely information for decision-making operations.

■ MIT successfully demonstrated OTH-GOLD track data exchanges with GCCS-J and its internal chat functionality to collaborate with coalition partners.

■ Visual display issues ranged from cluttered screens, small displays and insufficient contrasting color usage when displaying current track information.

■ The number of programs required to be opened and minimized created a burden for the operator and caused delays in providing timely information which negatively impacted the decision-making processes.

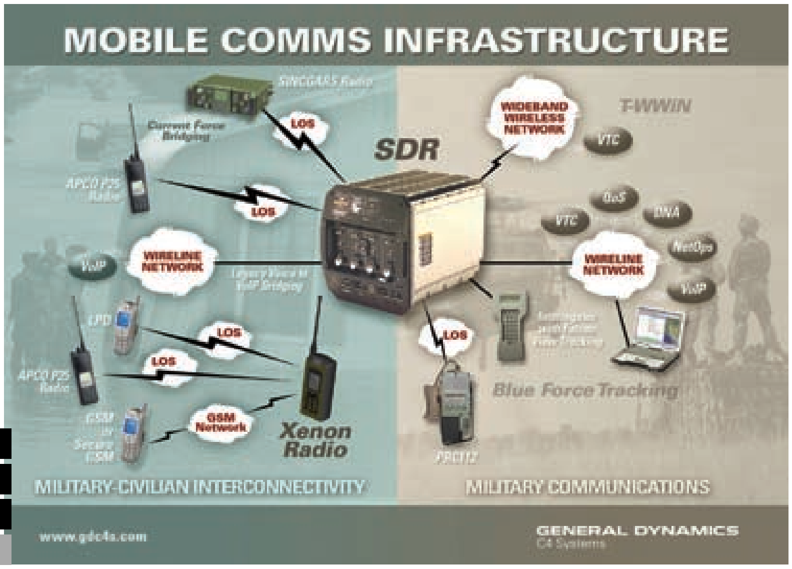
IT01.53

Coalition & Civil Agency Capable Wireless Information Transfer

1. COALITION C2 ● 5. NET-CENTRIC ENTERPRISE SERVICES ●

TRIAL OVERVIEW: Coalition and Civil Agency Capable Wireless Information Transfer System (C3WITS) is a Joint Tactical Radio System (JTRS)/Software Defined Radio (SDR) enabled system that provides; assured Blue Force Tracking, Common Situational Awareness Picture for both airborne and ground based command and control, Tactical Combat Net Radios (CNR) with range extension, and a Homeland Security Gateway. The system provides communication capabilities between dissimilar radios for DOD and HLS and secure video teleconferencing between wireless users or between wired and wireless users, enabling real-time interactive command and control as well as command and control, and communications (C3) capabilities between DOD/Civilian Agencies and local police and fire departments. The system can be used with either the embedded NSA Certified or external COMSEC.

SPONSORS: US Navy
TRIAL LOCATIONS: USEUCOM, USNORTHCOM, NSWC Dahlgren, SPAWAR,
TRIAL PARTNERS: None



WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING

ASSESSMEMT RESULTS:
During CWID 2006, the C3WITS Trial received Warfighter, Technical Interoperability, and Information Assurance assessments.

■ Successfully demonstrated CWID Objectives 1 and 5.

■ C3WITS securely connected many endpoint devices including diverse radios, cell phones, VoIP, and, wired and wireless workstations.

■ C3WITS successfully demonstrated a robust SDR System that was well-engineered and easy to use. Using NSA approved equipment, C3WITS securely bridged dissimilar radios, providing warfighters digital radio communications throughout the battlespace.

■ One detractor to the trial was that Trojan signatures were detected on several open ports as well as a vulnerability allowing Null sessions on the remote host.

■ Network performance monitors gave indications that network performance would be considerably dampened during use of the full production piece of this trial.

GO TO CD HOME PAGE

IT01.54

Coast Guard C2 (Deepwater Common Operational Picture)

1. COALITION C2 ●

TRIAL OVERVIEW: The Coast Guard Command and Control (CG-C2), part of the Integrated Deepwater System Program, provides interoperable command and control (C2) and establishes the foundations for integrating intelligence data across all deepwater aircraft, vessels and shore facilities. The system's core capabilities include a tactical display overview, deepwater portal, common operating picture, common collaboration tools, case file management, and automated status systems. CG-C2 delivers C4ISR capabilities, increasing the USCG's operational effectiveness and intra/agency communication by maximizing data and voice sharing among watchstanders, decision makers and operators. CG-C2 provides operational commanders the tactical awareness, planning and decision tools required to more effectively conduct missions.

SPONSOR: US Coast Guard
TRIAL LOCATIONS:
USNORTHCOM,
NSWC Dahlgren, SPAWAR
TRIAL PARTNERS: IT05.37

WARFIGHTER

TECHNICAL / INTEROPERABILITY

INFORMATION ASSURANCE

SYSTEMS ENGINEERING

GO TO CD TRIAL DIRECTORY

GO TO CD HOME PAGE

ASSESSMEMT RESULTS:
During CWID 2006, the CG-C2 Trial received Warfighter, Technical Interoperability, and Information Assurance assessments.

- CG-C2 successfully met CWID Objective 1 by providing Coast Guard track data from multiple sources throughout all operational levels (Commander to the various Sectors).
- The CG-C2 system successfully exchanged track data in OTH-Gold format with IT05.37 (JEBC2) and maritime tracks from HLD COP via CST, enhancing information presented on warfighter displays.
- CG-C2 shared geo-location track data between Federal Aviation Administration (FAA) Air Martime Operations Center (AMOC) and CG HQ (HLD/HLS COP) systems, providing C2 cohesion.
- CG-C2 provided the platform to share case files, intelligence alerts, force mix and asset allocation data with other HLS/HLD partners. CG-C2 fused Deepwater asset information into a single picture that provided real-time tactical awareness for USCG planning.

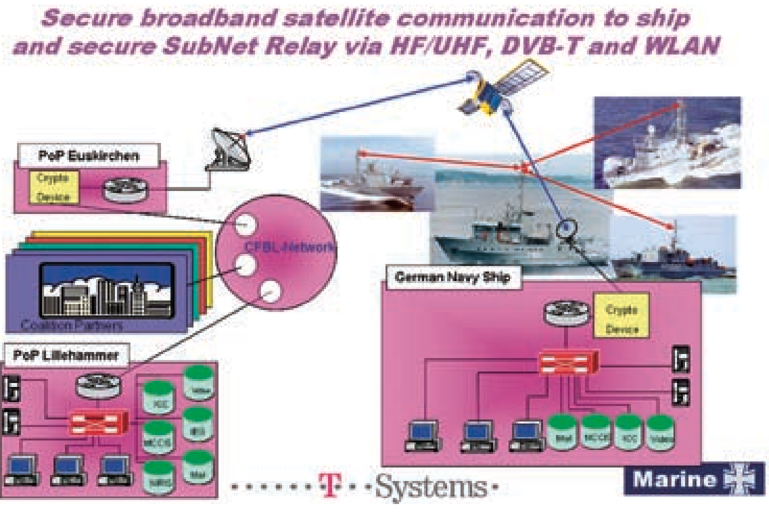
IT01.62

Mobile Forces Solution

1. COALITION C2 ● 4. CONTINUITY OF OPERATIONS ● 5. NET-CENTRIC ENTERPRISE SERVICES ●

TRIAL OVERVIEW: MobileForcesSolution (MOFS) is a distributed IP-Infrastructure with secure broadband satellite communication for MCCIS, ICC, ERP-System (SAP), VoIP and video conferencing. The remotely deployed Maritime Component Commander (MCC), communicates and/or shares relevant information with subordinates at sea or in theater using "SubNet Relay" in order to maintain situational awareness of ongoing movements and operations. MOFS provides secure communications redundancy for ships with satellite links and connectivity for disadvantaged ships without satellite access.

SPONSOR: Germany
TRIAL LOCATIONS:
SPAWAR, NATO
TRIAL PARTNERS: None



Secure broadband satellite communication to ship and secure SubNet Relay via HF/UHF, DVB-T and WLAN

WARFIGHTER

TECHNICAL / INTEROPERABILITY

INFORMATION ASSURANCE

SYSTEMS ENGINEERING

ASSESSMEMT RESULTS:
During CWID 2006, the MOFS Trial received Warfighter and Technical Interoperability assessments.

- MOFS successfully met CWID Objectives 1, 4 and 5.
- MOFS provided a sub-net relay and web portal for communication and secure data sharing between deployed units and shore installations, enhancing the CTF Commander's situational awareness and connectivity with deployed assets.
- Ships exchanged email, video, audio, and OTH-Gold track data with users on the CTF network using HF/UHF and IP over DVB-T and broadband satellite.
- The sub-net relay improved horizontal data access, fusion and integration, and improved horizontal information distribution by allowing four maritime assets to collaborate and function as a single COI. An established web portal allowed for improved vertical information distribution from deployed maritime assets to shore-based COIs.

GO TO CD HOME PAGE

IT01.63

IPC Multimedia Converged Communications Solution

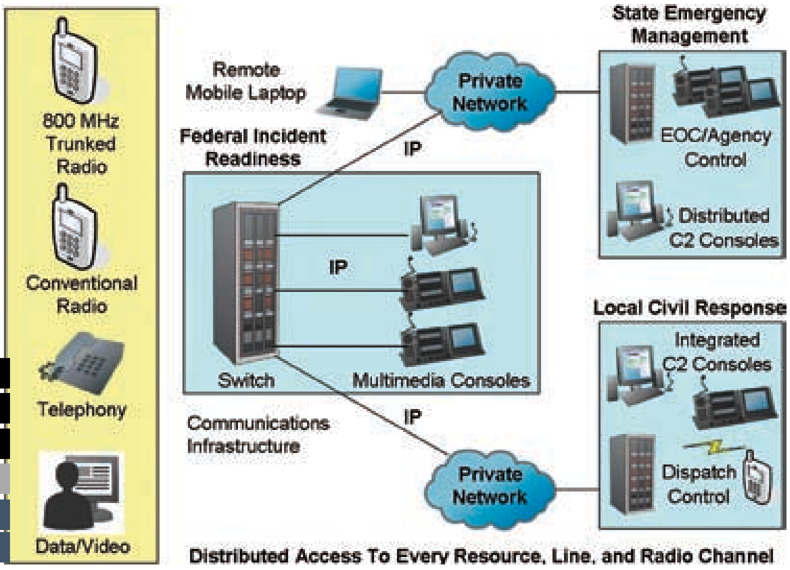
1. COALITION C2 ●

TRIAL OVERVIEW: The IPC Multimedia Converged Communications Solution (MCCS) is an IP-based audio multimedia communications platform enabling quick and efficient information collection, collaboration with stakeholders, and broadcast of an optimized response plan. IPC MCCS integrates mission-critical voice, data and video in a single command console. It enhances warfighter situational awareness by combining, separate, isolated systems and enabling seamless crosspatch across wireless and wired communications medium. The system simultaneously sends and receives data, video and voice as well as providing full recording capability. The IPC MCCS brings a unified approach to command and control facilitating better decisions and reducing the complexities associated with communicating these decisions to all concerned parties.

SPONSOR: Federal Emergency Management Agency (FEMA)
TRIAL LOCATIONS: USNORTHCOM, NSWC Dahlgren
TRIAL PARTNERS: None

WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING

GO TO CD TRIAL DIRECTORY
GO TO CD HOME PAGE



Distributed Access To Every Resource, Line, and Radio Channel

ASSESSMEMT RESULTS:
During CWID 2006, the IPC MCCS Trial received Warfighter and Technical Interoperability assessments.

■ MCCS was moderately successful in meeting CWID Objective 1. While MCCS successfully bridged the communications gaps between radios, telephones, and computers, MCCS experienced technical difficulties and reliability problems at multiple sites which kept it from showcasing its full potential.

■ MCCS could not view a CNN news feed on the MCCS console or receive broadcasts from another MCCS station and warfighters could not send/receive text alert messages via radio as originally planned.

■ Warfighters were concerned that MCCS was too complicated and needed enhancements to make the interface more intuitive.

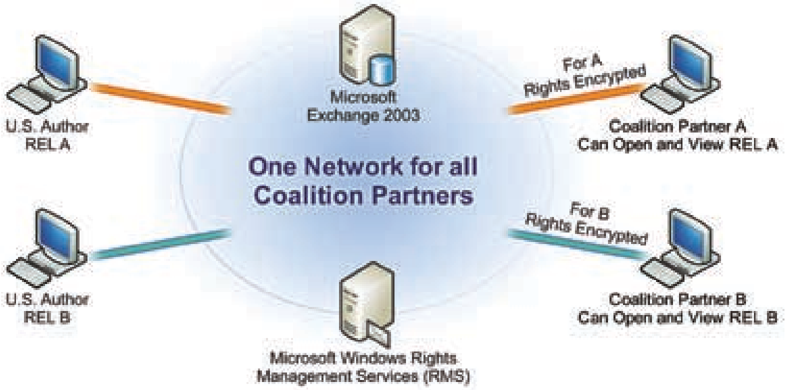
IT02.21

Multi National Coalition Security System

2. COALITION INFORMATION SHARING ● 5. NET-CENTRIC ENTERPRISE SERVICES ●

TRIAL OVERVIEW: The Multi National Coalition Security System (MNCSS) enables continuous control of email, documents and files for information sharing among different coalition forces communities in a single, common, secure network. Users select mandatory classification markings for newly created documents and emails and then using Microsoft's Rights Management Services (RMS), files are encrypted at the workstation and decrypted by the recipient. The encryption and decryption is based on the assigned classification markings and creates a robust environment for role and community-of-interest based information access. RMS enables digital rights assignment to control data files and emails and includes the ability to view, modify, print and distribute files. This capability operates within the familiar MS Office desktop environment.

SPONSOR: Canada
TRIAL LOCATIONS: Canada, NSWC Dahlgren, SPAWAR, Hanscom AFB, Australia, New Zealand, UK
TRIAL PARTNERS: None


Microsoft Exchange 2003
U.S. Author REL A
For A Rights Encrypted
Coalition Partner A Can Open and View REL A
One Network for all Coalition Partners
U.S. Author REL B
For B Rights Encrypted
Coalition Partner B Can Open and View REL B
Microsoft Windows Rights Management Services (RMS)

- Email and Documents are encrypted at workstation and decrypted by recipient
- Only authorized coalition partners can open and view files
- Data in transit is encrypted

WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING

ASSESSMEMT RESULTS:
During CWID 2006, the MNCSS Trial received Warfighter, Technical Interoperability, and Information Assurance assessments.

■ MNCSS successfully demonstrated CWID Objectives 2 and 5.

■ Warfighters marked emails and word documents with classification, releasability and precedence information and distributed the data horizontally and vertically within and between COIs.

■ A majority of the Warfighters agreed MNCSS capabilities provided a step forward in tightening the security of shared information.

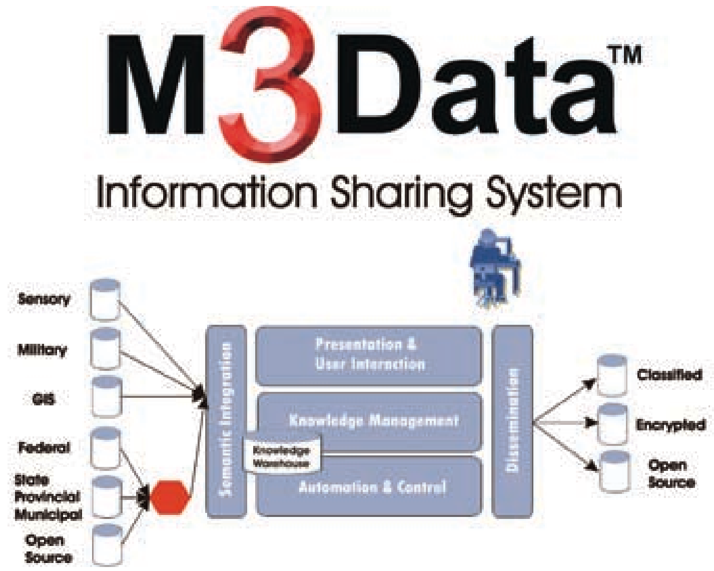
■ IA scans found open ports with no associations which could pose security risks. Other vulnerabilities detected included Null password on System Admin account, Terminal Services running, and Internet Control Message Protocol (ICMP) requesting Time Stamps.

IT02.24
M3Data Information Sharing System

1. COALITION C2 ● 5. NET-CENTRIC ENTERPRISE SERVICES ●

TRIAL OVERVIEW: M3Data Information Sharing System (M3Data ISS) provides a secure, intelligent middle-ware solution for Military, Intelligence, and Government applications. M3Data ISS delivers integrated command and control (C2) applications in a timely and flexible manner, simplifying inter-agency information sharing, interoperability, and contextual access enhancing situational awareness and decision-making. The system integrates multiple disparate systems with re-useable software, targeting the specific needs of command and control.

SPONSOR: Canada
TRIAL LOCATIONS:
Canada, UK
TRIAL PARTNERS: None



WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING

GO TO CD TRIAL DIRECTORY
GO TO CD HOME PAGE

ASSESSMEMT RESULTS:
During CWID 2006, M3Data ISS received Warfighter, Technical Interoperability and Information Assurance assessments.

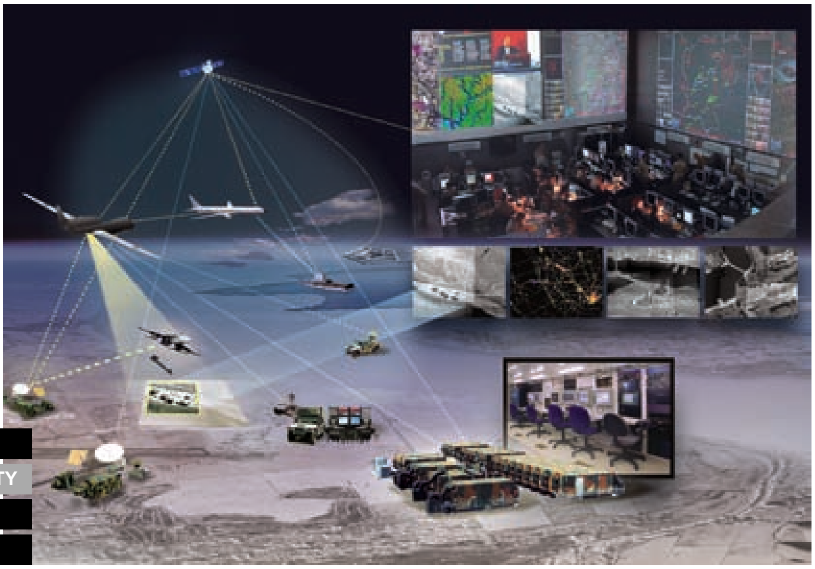
- M3Data successfully met CWID Objective 1 by providing the ability for rapid and agile integration of disparate knowledge bases and by providing secure access to those integrated knowledge bases.
- M3Data successfully demonstrated CWID Objective 5 by functioning as a middleware platform allowing data collection from multiple sources through a single web-based access point. Data sources included GCCS, Red Force Web-based Encyclopedia, simulated "MIDB" Server, file server with MS Word and PDF documents, and the SharePoint CWID document collaboration service.
- M3Data Agent added a new data file server to search and easily demonstrated creating a machine-to-machine link for improving the machine-to-human interface.

IT02.25
Distributed Common Ground System

2. COALITION INFORMATION SHARING ●

TRIAL OVERVIEW: DCGS transforms existing USAF DCGS stovepipe systems into open enterprise architecture and creates a worldwide net-centric DCGS systems consisting of all DCGS nodes working together as one single enterprise. DCGS is a globally integrated, distributed and collaborative information technology enterprise providing continuous on-demand full spectrum dominance intelligence brokering for American and Coalition forces. The environment provides physical and electronic distribution of Intelligence, Surveillance and Reconnaissance (ISR) data, process and systems. DCGS overcomes interoperability obstacles in Joint and Coalition environments by enabling posting of current data to the network for immediate use by analysts and warfighters. Integrated with other assets, DCGS improves battlespace situational awareness.

SPONSOR: Canada
TRIAL LOCATIONS: Canada, NSWC Dahlgren, SPAWAR, Hanscom AFB, UK
TRIAL PARTNERS: None



WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING

ASSESSMEMT RESULTS:
During CWID 2006, DCGS received a warfighter assessment and a SEIWG evaluation.

- DCGS successfully met CWID Objective 2 by providing merged situational awareness through a common operational picture. The trial provided real-time control and dynamic re-tasking of ISR production assets.
- The federation of DCGS nodes in U.S. and Canada demonstrated the distributed nature and the ability of the DCGS Integration Backbone to enable distributed access to ISR information and exploitation for information sharing between functional areas.
- Network power supply failures in Canada limited the amount of time the tool was used. Some warfighters in Canada indicated that many tool capabilities were not fully explored. However, they liked the parts of DCGS that they used, commenting that it worked well and was easy to use.

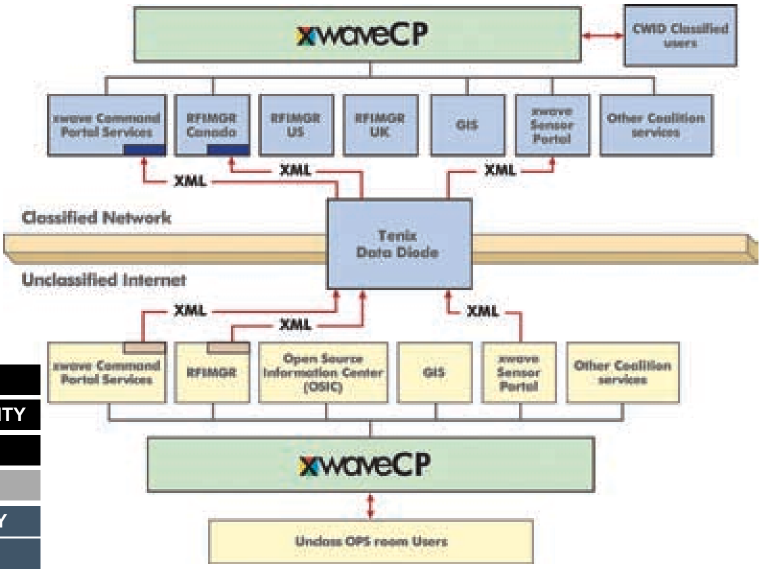
IT02.45

Command Center Portal Framework

2. COALITION INFORMATION SHARING ●

TRIAL OVERVIEW: Command Center Portal Framework, (CCPF) is a collection of applications that form the foundation and framework of a command and control (C2) Coordination Centre or Collaboration system. For CWID 2006, the CCPF incorporated xWaveCP, a situational awareness portal, Open Source Intelligence Centre (OSIC), and xWave Request for Information Manager (RFIM) into a single web based portal. The framework allowed coalition command staff to create, organize, share, discover, task and brief information about specific tasks. The framework supports extensive connectivity to systems and data, staff efficiency, collaborative planning and shared situational awareness.

SPONSOR: Canada
TRIAL LOCATIONS:
Canada, USNORTHCOM, Australia, New Zealand, UK
TRIAL PARTNERS: None



WARFIGHTER

TECHNICAL / INTEROPERABILITY

INFORMATION ASSURANCE

SYSTEMS ENGINEERING

GO TO CD TRIAL DIRECTORY
GO TO CD HOME PAGE

ASSESSMEMT RESULTS:
During CWID 2006, the CCPF Trial received Warfighter and Technical Interoperability assessments.

■ CCPF successfully achieved CWID Objective 2 by demonstrating portal technology to pass requests for information (RFIs).The portal was stable and most warfighters found it easy to use. However, some users thought the application could be streamlined to meet their operational needs.

■ CCPF successfully achieved its stated objective of coalition information sharing by providing the capability to manage request for information as well as provide access to structured knowledge via a web portal.

■ A useful feature of the tool was the inclusion of the RFI originators email in the RFI that allowed the user to contact the originator if more information was required.

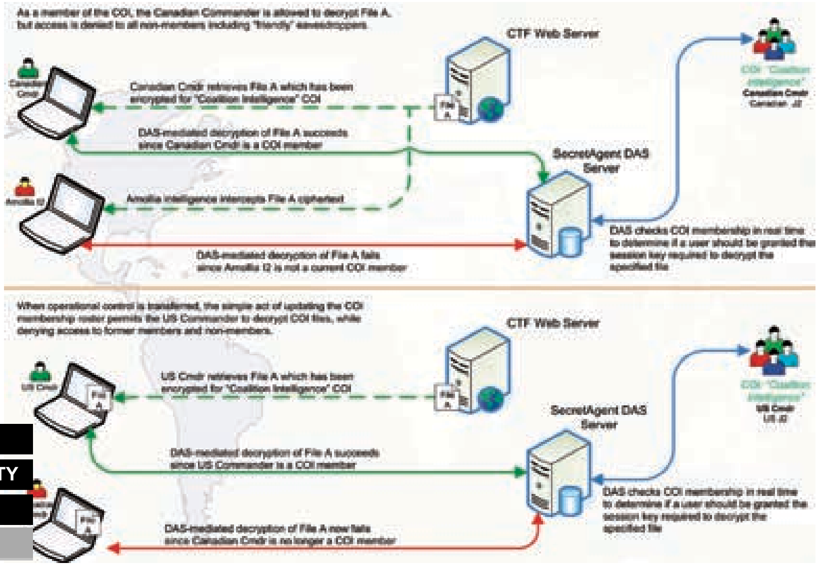
IT03.09

SecretAgent Document Access Servlet

5. NET-CENTRIC ENTERPRISE SERVICES ●

TRIAL OVERVIEW: Document Access Servlet (DAS) is a net-centric solution facilitating encrypted document sharing amongst authorized participants in a static or frequently changing environment and across command components. DAS allows updated document access rights to reflect real-time communities of interest (COIs), enhancing coalition information sharing in rapidly changing scenarios. DAS, in combination with SecretAgent, protects all types of files, at rest and/or during transmissions, independent of document storage and network transport mechanism employed by COIs. DAS expedites distribution of sensitive documents to COIs, is easy to use, and protects COI access changes in real-time. This solution provides for secure C2 relationships and improves the commanders' ability to securely receive and disseminate information.

SPONSOR: USEUCOM
TRIAL LOCATIONS:
USNORTHCOM, NSWC Dahlgren, SPAWAR, Hanscom AFB, Canada, New Zealand
TRIAL PARTNERS: None


As a member of the COI, the Canadian Commander is allowed to decrypt File A, but access is denied to all non-members including "friendly" eavesdroppers.

Canadian Cmdr retrieves File A which has been encrypted for "Coalition Intelligence" COI

DAS-mediated decryption of File A succeeds since Canadian Cmdr is a COI member

Amallia intelligence intercepts File A ciphertext

DAS-mediated decryption of File A fails since Amallia I2 is not a current COI member

DAS checks COI membership in real time to determine if a user should be granted the session key required to decrypt the specified file

When operational control is transferred, the simple act of updating the COI membership roster permits the US Commander to decrypt COI files, while denying access to former members and non-members.

US Cmdr retrieves File A which has been encrypted for "Coalition Intelligence" COI

DAS-mediated decryption of File A succeeds since US Commander is a COI member

DAS-mediated decryption of File A now fails since Canadian Cmdr is no longer a COI member

DAS checks COI membership in real time to determine if a user should be granted the session key required to decrypt the specified file

WARFIGHTER

TECHNICAL / INTEROPERABILITY

INFORMATION ASSURANCE

SYSTEMS ENGINEERING

ASSESSMEMT RESULTS:
During CWID 2006, the DAS Trial received Warfighter, Technical Interoperability, and Information Assurance assessments.

■ DAS successfully demonstrated CWID Objective 5 by providing the user a web portal interface to download, encrypt and decrypt files. DAS showed enhanced information assurance with the SecretAgent software, and improved vertical and horizontal information distribution between military and HLS/HLD COIs.

■ DAS was a user-friendly application requiring minimal training. Warfighters supported fielding in a military and HLS/HLD operational environment.

■ SecretAgent software of IT03.09 is NTTSP11 compliant based on FIPS 140 certificate and full evaluation of the crypto element by NSA.

■A detractor to the trial was that IA found open ports with no associations and Trojan signatures on several of the open ports. The open ports could create system vulnerabilities.

GO TO CD HOME PAGE

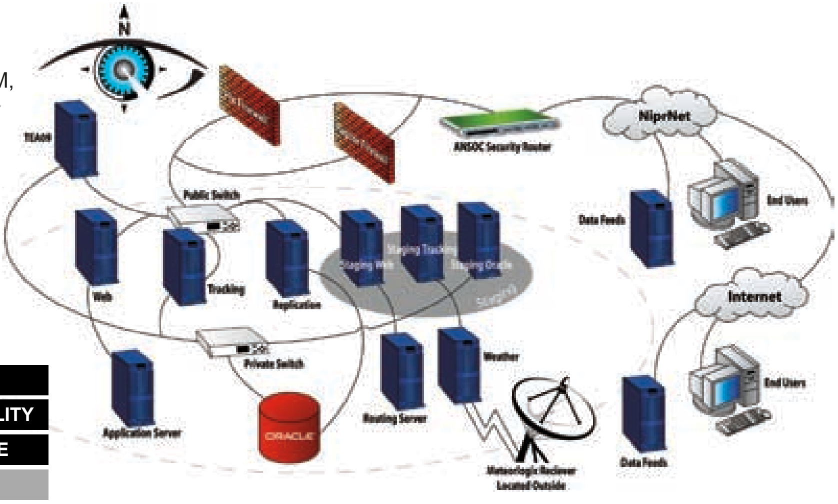
IT03.16

Intelligent Road/Rail Information Server

3. INTEGRATED LOGISTICS ● 5. NET-CENTRIC ENTERPRISE SERVICES

TRIAL OVERVIEW: Intelligent Road/Rail Information Server (IRRIS) is a fully secure, web accessible, geographic information system (GIS) that tracks critical supply chain assets and provides a common logistical picture for the shipment of goods. IRRIS is the only one-stop shop on the web that provides total asset visibility and in-transit visibility for shipping and logistics with real-time Global Positioning System (GPS) tracking. The system leverages open-architecture technology providing a simple mapping interface, which is as easy to use as Internet Explorer. IRRIS's suite of functionalities includes geospatial data and detailed mapping, asset tracking, vehicle routing, live data and alerts, alerts and notifications and plume analysis.

SPONSOR: US Army
TRIAL LOCATIONS: USEUCOM, USNORTHCOM, NSWC Dahlgren, SPAWAR
TRIAL PARTNERS: IT05.32, IT05.37



WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING
GO TO CD TRIAL DIRECTORY
GO TO CD HOME PAGE

ASSESSMEMT RESULTS:
During CWID 2006, IRRIS received Warfighter and Technical Interoperability assessments.

■ IRRIS successfully demonstrated Objective 3 by providing effective logistics information for personnel and supplies as well as providing clear logistical and transportation data via email and screen shots in a timely manner.

■ IRRIS successfully integrated with IT05.32, who provided a single signed-on to IRRIS web site, and was able to forward track data via OTH GOLD messages through IT05.37 to GCCS TOP COP satisfying CWID Objective 5.

■ Utilizing Total Asset Visibility (TAV) and In-Transit Visibility (ITV) functions IRRIS demonstrated transportation security, logistics and real-time tracking capabilities. Additionally, IRRIS passed Geo Imagery data via SMTP, SSL and SOAP to the TOPCOP via JEBC2.

■ Warfighters viewed IRRIS as a good tool for tracking surface vehicles, but recommended a software enhancement to differentiate the cargo between trucks.

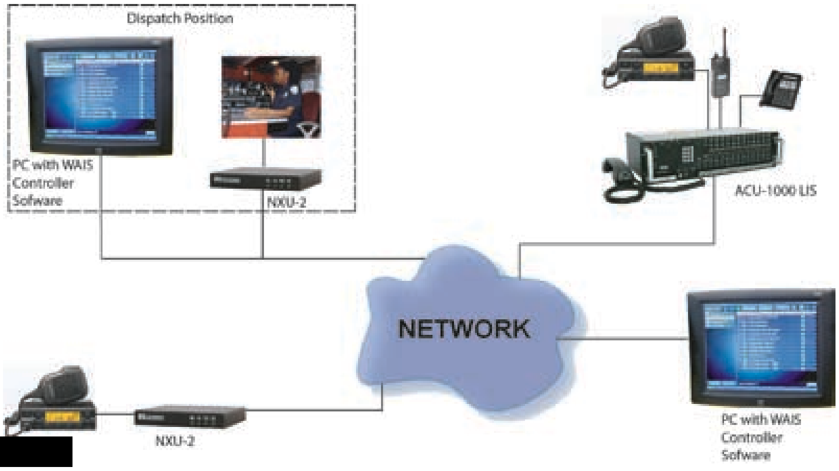
IT04.03

Wide Area Interoperability System and ACU-1000

1. COALITION C2 ● 5. NET-CENTRIC ENTERPRISE SERVICES

TRIAL OVERVIEW: The ACU-1000 and WAIS system enables collaboration and information dissemination between disparate communications systems and enhances seamless interoperability in a net-centric environment. The ACU-1000 seamlessly links radios, cellular, and land-line phones directly and over IP networks, providing local, regional, state, and wide-area interoperability. From homeland security to local public safety, from mission critical military application to the latest commercial requirement, the WAIS and ACU-1000 interoperability technology offers a robust communications solution for incident command management.

SPONSOR: USNORTHCOM
TRIAL LOCATIONS: USNORTHCOM
TRIAL PARTNERS: None



WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING

oIP/RoIP Compatibility
rowser-based configuration
etwork Connectivity

Enhanced Remote Control
Easier Setup
WAIS Enabled
P-25 Compatible

ASSESSMEMT RESULTS:
During CWID 2006, the WAIS and ACU-1000 Trial received Warfighter and Technical Interoperability assessments.

■ WAIS & ACU-1000 successfully met Objectives 1 & 5.

■ Utilizing VOIP technology WAIS & ACU-1000 bridged an existing local interoperability system to a wide area interoperability system enabling collaboration between DoD and Homeland Security/Homeland Defense (HLS/HLD)

■ WAIS and ACU-1000 allowed UHF (465 MHz)/VHF (170.650 MHz) radios, a Cellular phone and a laptop, using different frequencies, to communicate with each other improving vertical and horizontal voice information distribution.

■ WAIS and ACU-100 formed Talk Groups made up of all possible combinations of radios and devices that included adding a laptop and telephone to the communication chain. The laptop with PCNXU software was able to communicate with all radios (UHF and VHF) connected to WAIS.

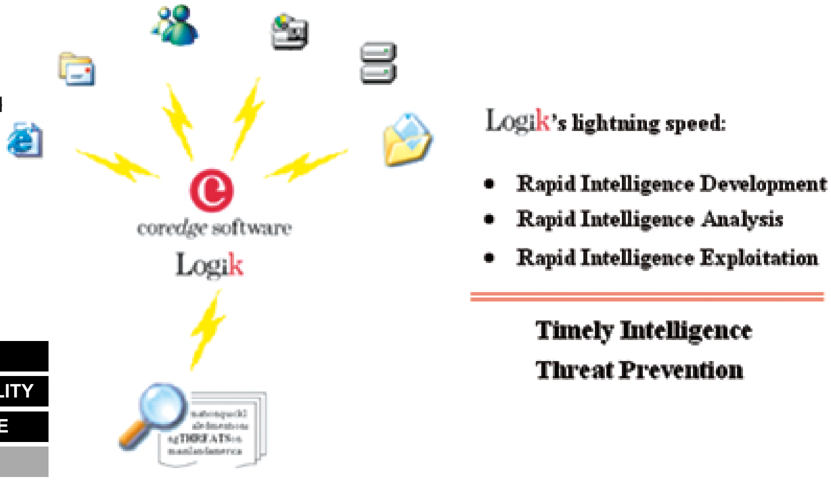
IT04.33

Logik v. 3.0 for Rapid Intelligence Analysis and Exploitation

4. CONTINUITY OF OPERATIONS ●

TRIAL OVERVIEW: Logik quickly processes large quantities of text data to support rapid intelligence analysis and exploitation that leads to timely and improved situational awareness for Combat Operations, Threat Assessment, Counter Intelligence, Counterterrorism, Intelligence Collection Planning, and Identification of Intelligence Gaps. The system provides superior keyword filtering enabling rapid intelligence information gathering and analysis. Logik processes information in eight languages including English, French, German, Dutch, Spanish, Portuguese, Japanese, and Arabic but additional languages can be added. Logik [machine] translates summaries and documents into seven languages including English, French, German, Italian, Japanese, Spanish and Portuguese.

SPONSOR: Canada
TRIAL LOCATIONS: Canada, USEUCOM, USNORTHCOM, NSWC Dahlgren, SPAWAR, UI
TRIAL PARTNERS: None


coredge software
Logik
Logik's lightning speed:
• Rapid Intelligence Development
• Rapid Intelligence Analysis
• Rapid Intelligence Exploitation
Timely Intelligence
Threat Prevention

WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING
GO TO CD TRIAL DIRECTORY
GO TO CD HOME PAGE

ASSESSMEMT RESULTS: During CWID 2006, the Logik Trial received Warfighter and Technical Interoperability assessments.

■ Logik successfully met Objective 4 by permitting users to sift through large volumes of information and pull out the pertinent data required to enhance the commander's ability to plan, communicate, and affect coalition operations.

■ Using Logik, users accessed libraries located on a server in San Diego, rapidly searched large quantities of information, identified the files' contents and retrieved only the predominant themes. This process saved valuable time when quick information analysis and prioritization was required.

■ The majority of properly trained users found Logik very intuitive. Overall, the trial received high warfighter remarks as those who saw the tools relevance were very impressed.

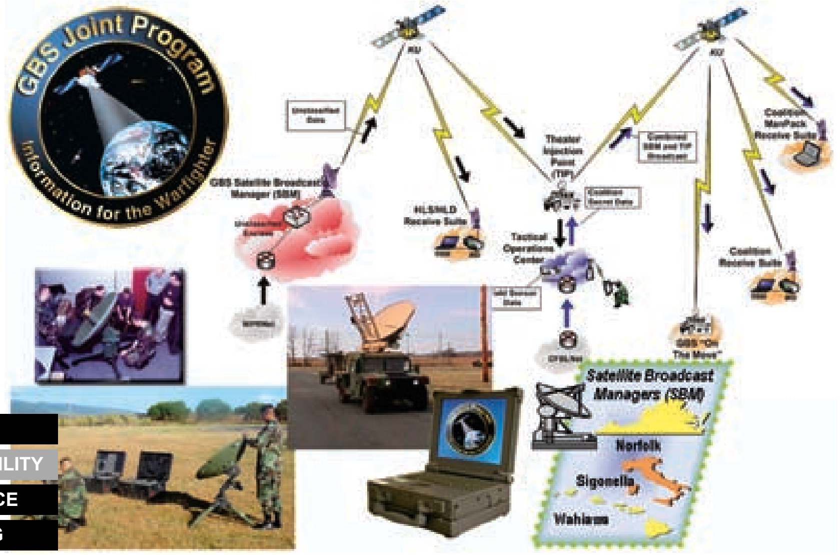
IT04.36

Global Broadcast Service

1. COALITION C2 ● 4. CONTINUITY OF OPERATIONS ● 5. NET-CENTRIC ENTERPRISE SERVICES ●

TRIAL OVERVIEW: The Global Broadcast Service (GBS), a fielded program of record, is a network-centric service extension of the Global Information Grid (GIG) and provides worldwide, high capacity, one-way transmission of video, imagery, intelligence and order of battle data. Data is sent to transportable Receive Suites (RS) or shipboard RS and used to support land or sea based forces in garrison, in transit and in theater. GBS added a new suite of capabilities and technologies that included a man-packable receive terminal and a prototype Theater Injection Point (TIP) supporting injection of tactical data. The TIP is a small rack-mounted, transportable GBS broadcast management system. TIP extends uplink capabilities to deployed warfighters and enables data broadcasts from disconnected or bandwidth constrained tactical operational centers.

SPONSOR: DISA
TRIAL LOCATIONS: USNORTHCOM, NSWC Dahlgren
TRIAL PARTNERS: IT05.37


GBS Joint Program
Information for the Warfighter
Unclassified Data
GBS Satellite Broadcast Manager (SBM)
HLS/HLD Receive Suite
Theater Injection Point (TIP)
Combined SBM and TIP Broadcast
Coalition Secret Data
Tactical Operations Center
Coalition ManPack Receive Suite
Coalition Receive Suite
GBS "On The Move"
Satellite Broadcast Managers (SBM)
Norfolk
Sigonella
Wahiawa

WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING

ASSESSMEMT RESULTS: During CWID 2006, the GBS Trial received a Warfighter assessment and a SEIWG evaluation.

■ GBS had equipment and technical issues prior to execution that prevented demonstrations of their new capabilities. (Other than Secret Enclave and Communication On The Move [COTM])

■ With the aid of a partnering trial, GBS streamed video data from unclass to the CTF enclave in a Net Centric environment but the video quality was inconsistent.

■ The Man-Packable RBM prototype was a CWID highlight and is ready for immediate procurement and delivery.

■ GBS received, and broadcast data (e.g. weather, intel, video) successfully between Dahlgren to USNORTHCOM on the HLS/HLD network demonstrating objectives 1, 4 and 5.

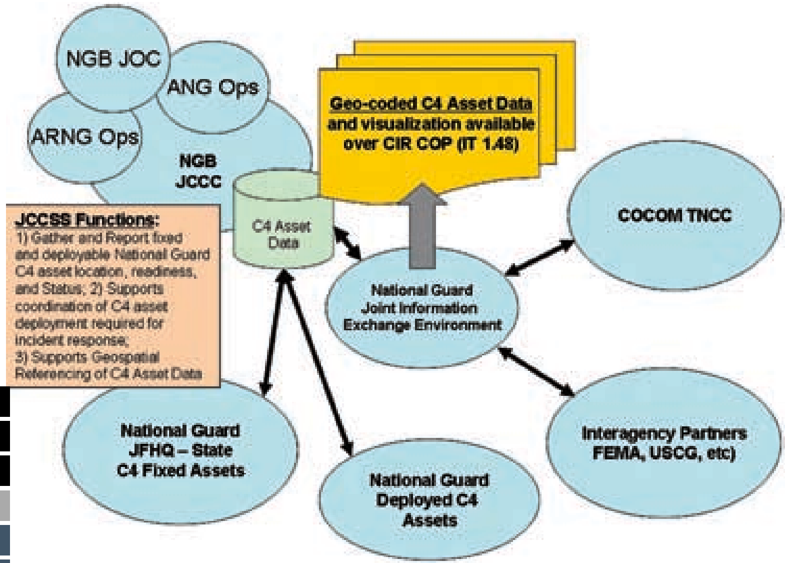
GO TO CD HOME PAGE

IT04.46
Joint C4 Coordination Support System

4. CONTINUITY OF OPERATIONS ●

TRIAL OVERVIEW: Joint C4 Coordination Support System (JCCSS) provides the capability to gather and report fixed and deployable National Guard C4 asset locations, readiness and status. JCCSS enables continuous situational awareness of assets enabling Homeland Security and Homeland Defense decision makers and partners to coordinate and position communications assets across a region in response to emergencies. JCCSS capabilities developed were part of an overall Joint Information Exchange Environment (JIEE) requirement identified in the USNORTHCOM - National Guard Bureau Joint CONUS communications Support Environment (JCCSE) Concept for Joint C4.

SPONSOR: National Guard Bureau
TRIAL LOCATIONS: USNORTHCOM, NSWC Dahlgren
TRIAL PARTNERS: IT01.48, IT05.47


NGB JOC
ANG Ops
ARNG Ops
NGB JCCC
C4 Asset Data
Geo-coded C4 Asset Data and visualization available over CIR COP (IT 1.48)
COCOM TNCC
JCCSS Functions:
1) Gather and Report fixed and deployable National Guard C4 asset location, readiness, and Status; 2) Supports coordination of C4 asset deployment required for incident response;
3) Supports Geospatial Referencing of C4 Asset Data
National Guard Joint Information Exchange Environment
National Guard JFHQ – State C4 Fixed Assets
National Guard Deployed C4 Assets
Interagency Partners FEMA, USCG, etc)

WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING
GO TO CD TRIAL DIRECTORY
GO TO CD HOME PAGE

ASSESSMEMT RESULTS:
During CWID 2006, JCCSS received Warfighter and Technical Interoperability assessments.

■ JCSS focused on tracking NGB incident area C4 assets and successfully met Objective 4 capabilities by sending data layers to the HLD COP Manager.

■ On JCSS Guard Knowledge Online portal, incident responders used the NGB Layer Editor to create data layers outlining locations of C4 assets. This information was viewed on NASA WorldWind and accessed through the Joint Operations Environment (JOE). The Layer Editor was also used to enter responders to an incident. The resulting tracks were viewed on the NASA WorldWind at USNORTHCOM.

■ Supported the sharing of C4 asset location and readiness to promote continuity of C4 operations from incident area to state and national levels.

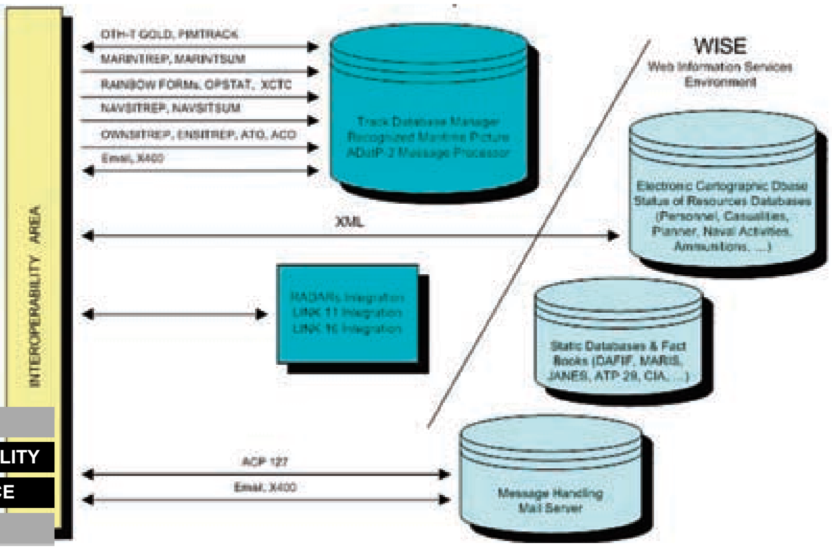
■ Provided decision support relative to operating conditions (i.e., inform decision makers on remote deployments based on available incident area communications).

IT04.61
Maritime Command and Control Information System-Italy

1. COALITION C2 ●

TRIAL OVERVIEW: The Italian Maritime Command & Control Information System (MCCIS-I) allows the Maritime Commanders and their Staffs to automatically acquire, analyze, display, and maintain large quantities of information. MCCIS-I electronically processes multiple source data, displays the information in various Command and Control (C2) applications and provides users the ability to manipulate the data for Strategic, Operation, and Tactical Command decision makers. For CWID 2006, MCCIS-I interoperated and integrated with the US Joint Global Command and Control System (GCCS-J) and the Maritime Global Command and Control System (GCCS-M).

SPONSOR: Italy
TRIAL LOCATIONS: NATO, SPAWAR
TRIAL PARTNERS: None


INTEROPERABILITY AREA
OTH-T GOLD, PIMTRACK
MARINTREP, MARINTSUM
RAINBOW FORMs, OPSTAT, XCTC
NAVSITREP, NAVSITSUM
OWNSITREP, ENSITREP, ATO, ACO
Email, X400
Track Database Manager
Recognized Maritime Picture
ADatP-3 Message Processor
WISE
Web Information Services Environment
Electronic Cartographic Dbase
Status of Resources Databases (Personnel, Casualties, Planner, Naval Activities, Ammunitions, ...)
XML
RADARs Integration
LINK 11 Integration
LINK 16 Integration
Static Databases & Fact Books (DAFIF, MARIS, JANES, ATP 29, CIA, ...)
ACP 127
Email, X400
Message Handling
Mail Server

WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING

ASSESSMEMT RESULTS:
During CWID 2006, the MCCIS-I Trial received a Technical Interoperability assessment.

■ MCCS/Italy successfully exchanged data with GCCS and demonstrated Joint Command and Control capabilities from Objective 1.

■ MCCS/Italy successfully provided Recognize Maritime Picture (RMP), Message Text Format (MTF), data and email exchange, testing the new release (5.1) capabilities to be fully interoperable and integrated with other C4I systems within NATO and Coalition Nations.

■ GCCS-J successfully received and displayed the RMP on the Top COP. This was an automated process whereas the Italian trial sent an email with the RMP embedded directly to the GCCS-J between USEUCOM and SPAWAR, San Diego.

IT05.06

Visual Assistant for Information Assurance

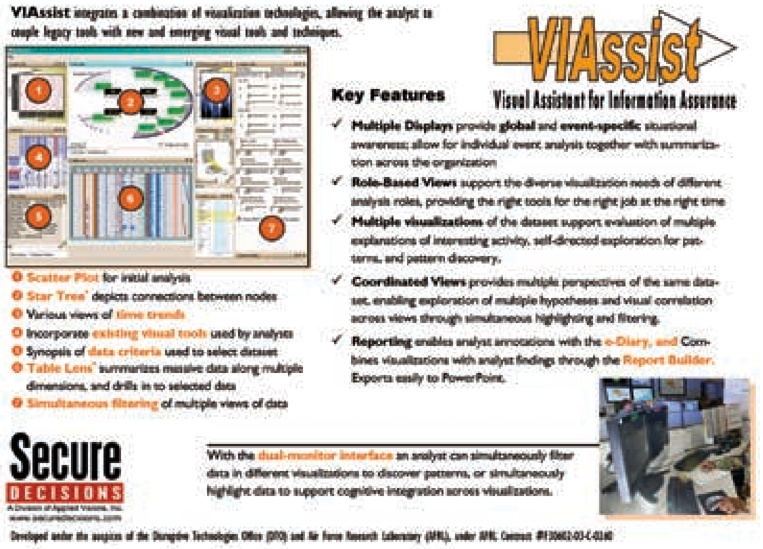
1. COALITION C2 ● 2. COALITION INFORMATION SHARING ● 5. NET CENTRIC ENTERPRISE SERVICES ●

TRIAL OVERVIEW: Visual Assistant for Information Assurance (VIAssist), an integrated visualization system, integrates best-of-breed tools transforming arcane network security data into relevant statistical and relational graphics. VIA Assist supports information assurance (IA) analysts and operational decision makers to increase cyberspace situational awareness (SA) and improve decisions. Network operators review and analyze data from disparate IA/Computer Network Defense (CND) systems and analyze massive volumes of network/cyber security data to determine the sources and forms of critical events threatening mission survivability. VIAssist provides global SA as well as detailed awareness of individual critical events. Operators view IA data from multiple sensors and graphically depict its data source from multiple perspectives.

SPONSOR: US Air Force
TRIAL LOCATIONS:
NSWC Dahlgren, New Zealand
TRIAL PARTNERS: None

WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING

GO TO CD TRIAL DIRECTORY
GO TO CD HOME PAGE



VIAssist integrates a combination of visualization technologies, allowing the analyst to couple legacy tools with new and emerging visual tools and techniques.

VIAssist
Visual Assistant for Information Assurance

1. Scatter Plot for initial analysis
2. Star Tree™ depicts connections between nodes
3. Various views of time trends
4. Incorporate existing visual tools used by analysts
5. Synopsis of data criteria used to select dataset
6. Table Lens™ summarizes massive data along multiple dimensions, and drills in to selected data
7. Simultaneous filtering of multiple views of data

Key Features

- ✓ **Multiple Displays** provide **global** and **event-specific** situational awareness; allow for individual event analysis together with summarization across the organization
- ✓ **Role-Based Views** support the diverse visualization needs of different analysis roles, providing the right tools for the right job at the right time
- ✓ **Multiple visualizations** of the dataset support evaluation of multiple explanations of interesting activity, self-directed exploration for patterns, and pattern discovery.
- ✓ **Coordinated Views** provides multiple perspectives of the same dataset, enabling exploration of multiple hypotheses and visual correlation across views through simultaneous highlighting and filtering.
- ✓ **Reporting** enables analyst annotations with the e-Diary, and Combines visualizations with analyst findings through the Report Builder. Exports easily to PowerPoint.

Secure DECISIONS
A Division of Applied Visions, Inc.
www.securedecisions.com

With the dual-monitor interface an analyst can simultaneously filter data in different visualizations to discover patterns, or simultaneously highlight data to support cognitive integration across visualizations.

Developed under the auspices of the Disruptive Technologies Office (DTO) and Air Force Research Laboratory (AFRL), under AFRL Contract #F30602-03-C-0240

ASSESSMEMT RESULTS:
During CWID 2006, VIAssist received Warfighter and Technical Interoperability assessments.

■ VIAssist successfully met CWID objectives 1, 2 and 5, providing user friendly, easy-to-interpret visual displays of external and internal network operations.

■ The VIAssist dashboard provided a concise overview of network traffic and threats, providing analysts over 30 distinct tools to interpret IP address traffic and create a comprehensible report for commanders to collaborate and disseminate information to COIs.

■ VIAssist's visual demonstration permitted commanders to effectively brief network vulnerabilities and threats to personnel of varying levels of expertise, providing clear situational awareness of computer network defense (CND).

■ VIA toolkit successfully analyzed data to filter out connections, analyzed data to/from .mil domain to IP addresses deemed unusual, and provided a situational awareness briefing transmitted via email.

IT05.13

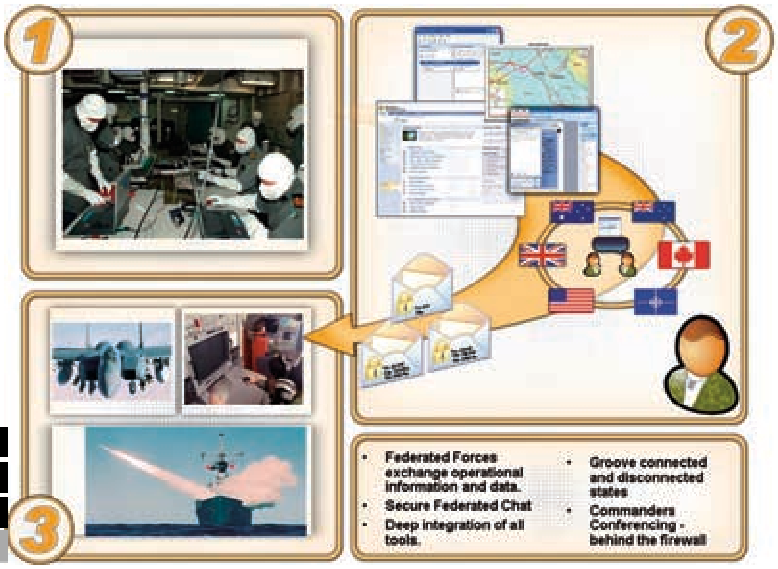
Coalition Command Collaboration Services

1. COALITION C2 ● 4. CONTINUITY OF OPERATIONS ●

TRIAL OVERVIEW: Coalition Command Collaboration Services (CCCS) is an integrated suite of collaboration tools and an enabling platform for integrating C4ISR applications hosted within SharePoint (e.g. XML, SOAP, using web parts, and .net patterns and practices). CCCS focuses on improving integration with the next generation information (Windows Vista, Office 12, SharePoint Portal & Groove Virtual Office) capabilities from Microsoft to produce a Command and Control (C2) console that adapts to integrating data from the edge of the network (e.g. weapons and sensors). CCCS demonstrates a federated security infrastructure information exchange between Military, Coalition, State and Federal Statuary organizations. CCCS provides efficiencies in bandwidth utilization, application integration, secure federated data sharing, and enhanced data protection.

SPONSOR: Australia
TRIAL LOCATIONS: Australia, Canada, New Zealand
TRIAL PARTNERS: None

WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING



- Federated Forces exchange operational information and data.
- Secure Federated Chat
- Deep integration of all tools.
- Groove connected and disconnected states
- Commanders Conferencing - behind the firewall

ASSESSMEMT RESULTS:
During CWID 2006, the CCCS Trial received Warfighter and Technical Interoperability assessments.

■ CCCS successfully CWID Objectives 1 and 4 by demonstrating an enhanced collaboration environment featuring an integrated suite of collaboration and office tools, allowing operational information exchange between federated forces in an easy (familiar) fashion.

■ Using the Groove virtual workspace within its collaboration tools, CCCS successfully demonstrated remote Microsoft Word and/or PowerPoint file sharing. The data type/format/transport mechanism for data exchanges included Text/XML/SOAP.

■ Additionally, CCCS demonstrated chat and telephone conferencing within its collaboration tools. The data type/format/transport mechanism for data exchanges included Voice/SIMP Chat/SOAP and Chat/Chat/SIP over TLS.

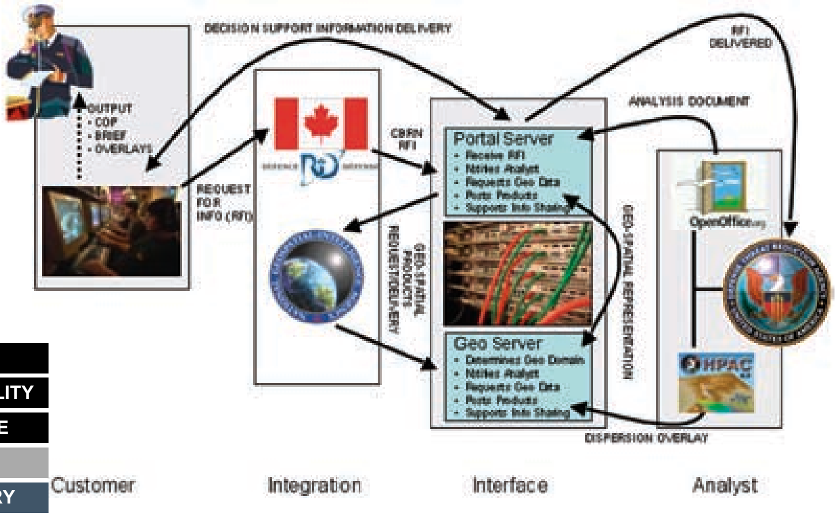
GO TO CD HOME PAGE

IT05.17
WMD Collaborative Advisory Response System

5. NET CENTRIC ENTERPRISE SERVICES ●

TRIAL OVERVIEW: The Weapons of Mass Destruction Collaborative Advisory Response System (WMD CARS) provides the Department of Defense (DOD), Homeland Security/Homeland Defense (HLS/HLD), and Coalition partners an unimpaired information-sharing tool in the event of a WMD occurrence. WMD CARS is a multi-use open-framework resource for deliberate and crisis action planning at strategic and operational levels. WMD CARS fuses dissimilar information and distributes critical information to the strategic decision maker to support consequence management, force protection, and military assistance to civil authorities in the event of hostile chemical, biological Radiological, and nuclear (CBRN) events.

SPONSOR: DTRA
TRIAL LOCATIONS:
USEUCOM, USNORTHCOM, Australia
TRIAL PARTNERS: None



WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING
GO TO CD TRIAL DIRECTORY
GO TO CD HOME PAGE

ASSESSMEMT RESULTS:
During CWID 2006, the WMD CARS Trial received Warfighter and Technical Interoperability assessments.

■ WMDCARS successfully satisfied its primary objective by providing users a means of observing, creating and then forwarding information to interfacing systems. Utilizing an open portal URL users could view graphic and textual data types, text documents, Power Point Documents, and GCCS (OTH-Gold) tracks.

■ The dynamic mapping product provided detailed data for CBRNE events and their potential effects including the WMD CARS plume on the USNORTHCOM HLD COP.

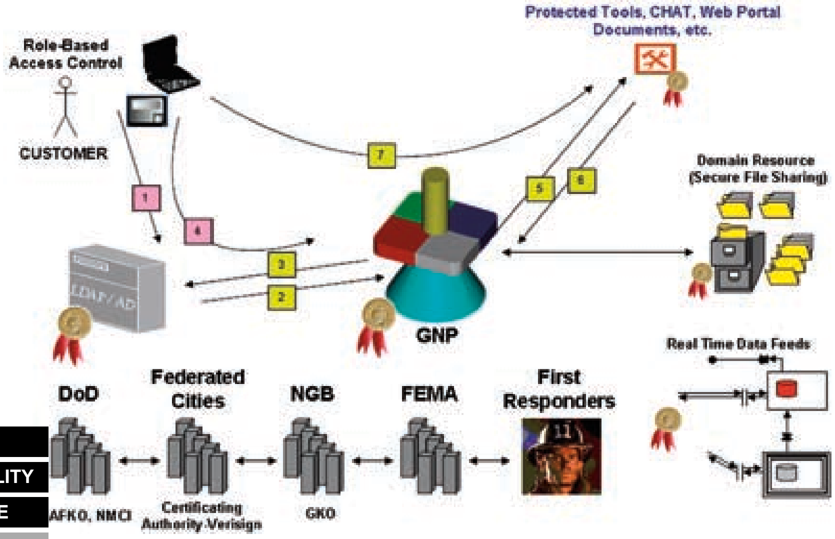
■ Warfighters effectively analyzed the data and made appropriate decisions towards CBRNE events. The system also provided quick updates to the local commander, increasing his overall situational awareness.

IT05.32
Guard Net Portal

1. COALITION C2 ● 5. NET CENTRIC ENTERPRISE SERVICES ●

TRIAL OVERVIEW: The GuardNet Portal (GNP) is a web-based tool providing role-based access and a single sign-on to communications media, tools such as chat, Voice over IP (VoIP), and documents. GNP acts a virtual switch linking those with data to those who need the data. It is easy to use and allows access to diverse tools securely; data and tool owners maintain control.

SPONSOR: US Navy
TRIAL LOCATIONS:
USEUCOM, USNORTHCOM, NSWC Dahlgren, SPAWAR
TRIAL PARTNERS: IT03.16, IT05.37


Protected Tools, CHAT, Web Portal Documents, etc.
Role-Based Access Control
CUSTOMER
1
2
3
4
5
6
7
LDAP/AD
GNP
Domain Resource (Secure File Sharing)
Real Time Data Feeds
DoD
Federated Cities
NGB
FEMA
First Responders
AFKO, NMCI
Certificating Authority-Verisign
GKO

WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING

ASSESSMEMT RESULTS:
During CWID 2006, the GNP Trial received Warfighter, Technical Interoperability, and Information Assurance assessments.

■ GNP users experienced technical difficulties at various sites throughout CWID 2006, leading to partially satisfying objectives 1 and 5. Warfighters commended the trials ideas were intriguing but system reliability and not so user- friendly interfaces limited their ability to successfully operate it.

■ GNP successfully demonstrated a single sign-on system with users logging into JFHQ workstations. Once logged into GNP, users accessed a partner trial IT03.16 IRRIS and GNP Chat without a new login process. While multiple single sign-on methods (JFHQ workstation, web-enabled cell phone, WiFi, PDA & CAC) were advertised, only the JFHQ workstation and PDA methods were utilized.

■ IA scans successfully validated GNP's PKI Certification denials but a detractor to the trial was that open ports with no associations were found which created vulnerabilities.

GO TO CD HOME PAGE

IT05.37

Joint Effects Based Command and Control

1. COALITION C2 ● 2. COALITION INFORMATION SHARING ● 3. INTEGRATED LOGISTICS ● 5. NET-CENTRIC ENTERPRISE SERVICES ●

TRIAL OVERVIEW: Joint Effects Based Command and Control (JEBC2) system provides an integrated architecture for Coalition, Joint, Federal and Civil Commanders, and analysts to share C2 information for planning, execution, and consequence management. JEBC2 consists of a Multi-level Security Information Infrastructure (MI2), a Warfighter Machine Interface (WMI) capability, and an Information Management (IM) capability. The WMI capability integrates mission applications into a common display while the IM capability brokers data in a Network Centric environment. The MI2 infrastructure combines information management and information assurance technologies allowing civil, government, and military communities to securely share information in real-time between classified and unclassified networks.

SPONSOR: USNORTHCOM
TRIAL LOCATIONS: USEUCOM, USNORTHCOM, SPAWAR, Canada
TRIAL PARTNERS: IT01.20, IT01.54, IT03.16, IT04.36, IT05.32, IT05.51

BOEING
Warfighter Machine Interface
Command and Control Applications
Multilevel Security and Information Management
Demonstrating a Network-Centric Architecture That Facilitates Information Sharing and Command & Control

WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING

GO TO CD TRIAL DIRECTORY
GO TO CD HOME PAGE

ASSESSMEMT RESULTS:
During CWID 2006, JEBC2 received Warfighter, Technical Interoperability, and Information Assurance assessments.

- Objectives 1, 2, and 5 were met, however, Objective 3 was not met as JEBC2 did not create or provide any logistics data on its own.
- JEBC2 demonstrated varying technology integrations on the WMI via dynamic information sharing and provided alerts from low to high security domains with one-way data diode. Alerts propagated were successful.
- JEBC2 demonstrated ability to collect track, video, and logistical data in a Net Centric environment for display on WMI as well as distributing data among other trials and systems. Some warfighters experienced data display and access inaccuracies.
- JEBC2 successfully demonstrated chat interoperability between XMPP and MIRC chat protocols.
- A detractor to the trial was that open ports with no associations were identified which created vulnerabilities.

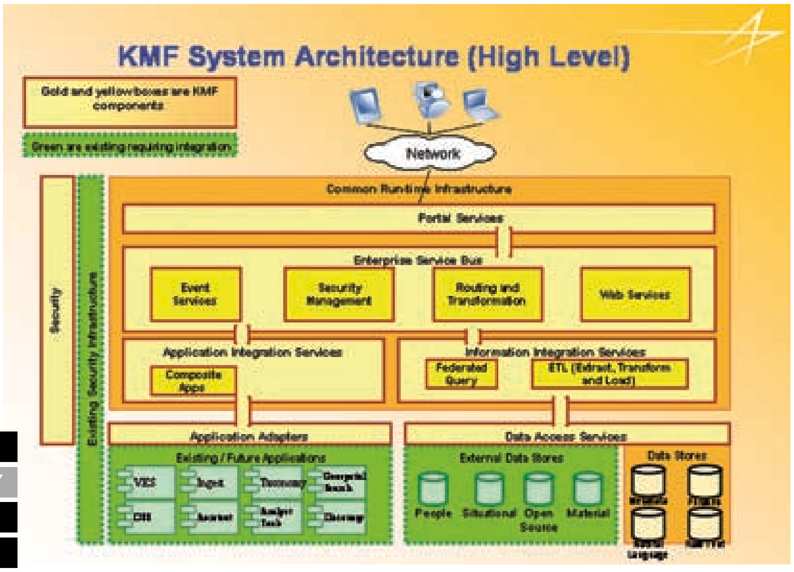
IT05.41

Knowledge Management Framework

5. NET CENTRIC ENTERPRISE SERVICES ●

TRIAL OVERVIEW: Knowledge Management Framework (KMF) provides a data/information centric architecture integrating various sources of information for analysis in a web based, standard environment. The KMF framework integrates several knowledge analysis and exploitation tools under a common portal. Users/analysts access, discover, and exploit multiple data sources and quickly develop tailored intelligence products for tactical and strategic operations. The main components of the system are the Ingest and Exploitation System, Metadata Repository, Knowledge Extraction Tools, Integrated Collaboration and Federated and Geospatial Search.

SPONSOR: Canada
TRIAL LOCATIONS: Canada
TRIAL PARTNERS: None


KMF System Architecture (High Level)
Gold and yellow boxes are KMF components
Green are existing requiring integration
Network
Common Runtime Infrastructure
Portal Services
Enterprise Service Bus
Event Services
Security Management
Routing and Transformation
Web Services
Application Integration Services
Composite Apps
Information Integration Services
Federated Query
ETL (Extract, Transform and Load)
Security
Existing Security Infrastructure
Application Adapters
Existing / Future Applications
Ingest
Taxonomy
Geospatial Search
Analyst Tools
Data Access Services
External Data Stores
People
Situational
Open Source
Material
Data Stores

WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING

ASSESSMEMT RESULTS:
During CWID 2006, the KMF Trial received Warfighter assessment and a SEIWG evaluation.

- Successfully demonstrated Objective 5 capabilities during CWID execution.
- While KMF's user base was very small (Canada only), warfighters that used the trial felt that KMF supported their tasks very well. Once familiar with the tools of the suite, KMF greatly accelerated the data discovery process.
- KMF warfighters created reports and knowledge products to satisfy RFIs. The KMF collaborative tool allowed warfighters to track and share documents and images with the ability to annotate and store comments with each product.

GO TO CD HOME PAGE

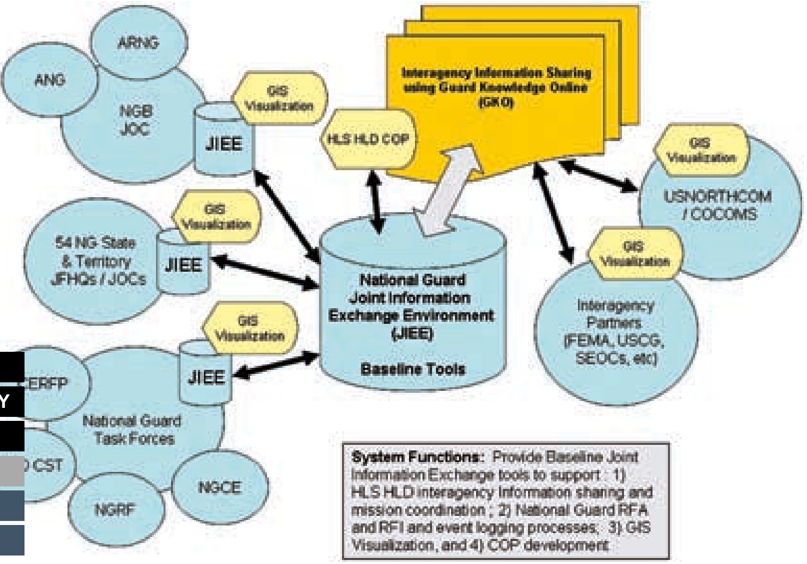
IT05.47

HLS/HLD Collaborative Information Exchange Environment

5. NET CENTRIC ENTERPRISE SERVICES ●

TRIAL OVERVIEW: Homeland Security/Homeland Defense Collaborative Information Exchange Environment (HLS/HLD CIEE) demonstrates a joint information exchange environment supporting inter-agency situational awareness, National Guard (NG) vertical and horizontal incident information sharing as well as Request for Information (RFI) and Request for Assistance (RFA). CIEE provides tools supporting interagency information sharing and mission coordination, NG RFA and RFI and event logging processes, and Global Information System (GIS) visualization and common operational picture (COP) development. These capabilities were developed as part of an overall Joint Information Exchange Environment (JIEE) requirement identified in the USNORTHCOM - NGB Joint CONUS communications Support Environment (JCCSE) Concept for Joint C4.

SPONSOR: National Guard Bureau
TRIAL LOCATIONS: USNORTHCOM, NSWC Dahlgren
TRIAL PARTNERS: IT01.48, IT04.46


ARNG
ANG
NGB JOC
JIEE
GIS Visualization
HLS HLD COP
Interagency Information Sharing using Guard Knowledge Online (GKO)
GIS Visualization
USNORTHCOM / COCOMS
54 NG State & Territory JFHQs / JOCs
JIEE
GIS Visualization
National Guard Joint Information Exchange Environment (JIEE)
Baseline Tools
GIS Visualization
Interagency Partners (FEMA, USCG, SEOCs, etc)
GIS Visualization
CERFP
JIEE
National Guard Task Forces
CST
NGCE
NGRF

System Functions: Provide Baseline Joint Information Exchange tools to support : 1) HLS HLD interagency Information sharing and mission coordination ; 2) National Guard RFA and RFI and event logging processes; 3) GIS Visualization, and 4) COP development

WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING
GO TO CD TRIAL DIRECTORY
GO TO CD HOME PAGE

ASSESSMEMT RESULTS:
During CWID 2006, the HLS/HLD CIEE Trial received Warfighter and Technical Interoperability assessments.

■ HLS/HLD CIEE successfully met Objective 5 by creating the JOE portal which set-up an information exchange environment for IT01.48 and IT04.46. Two distinct NGB web based tools, the JIEE tool and the Joint Operations Environment (JOE) tool in addition to CWID core services provided the information exchange mechanism.

■ NG personnel used the JIEE tool to exchange information within the NG. The JOE tool enabled other agencies, such as USNORTHCOM, to access incident logs, receive RFIs, and view NGB assets.

■ HLS/HLD CIEE enabled incident response information sharing such as SITREPS, OPPLANS, alerts, and COP data within States or across States (horizontal information dissemination) and from incident areas to National Operations Centers (i.e. USNORTHCOM -vertical information dissemination).

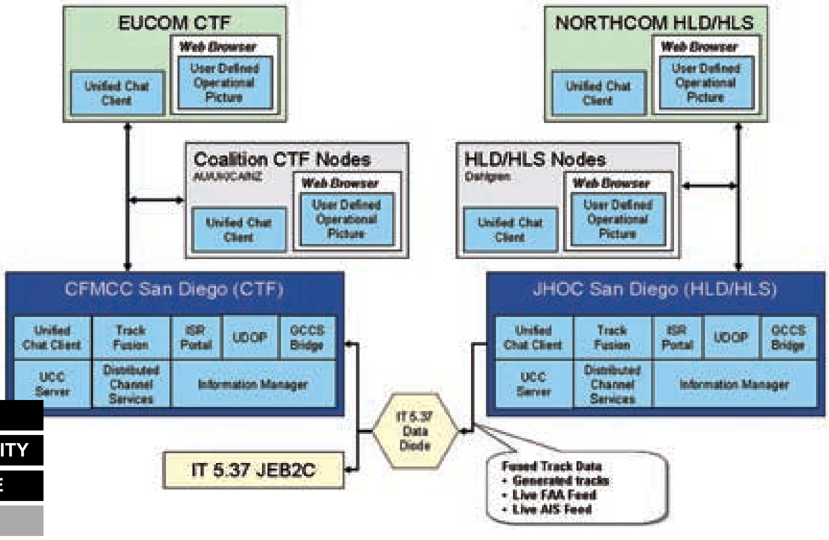
IT05.51

FORCEnet Distributed Channel Services

1. COALITION C2 ● 5. NET CENTRIC ENTERPRISE SERVICES ●

TRIAL OVERVIEW: FORCEnet Distributed Channel Services (FnDCS) supports timely decision-making across nets such as the Internet and provides interoperability with other service-oriented architectures even in bandwidth-constrained operations. Using distributed channel services and semantic web features and functions, FNDCS enables coalition collaboration with context, time and space relations to (1) improve information assurance, (2) improve horizontal data access, fusion and integration and (3) improve vertical and horizontal information distribution in maritime and homeland defense situations. Persistent FnDCS chat and text-to-voice intelligent notification functions aid in continuity of operations.

SPONSOR: US Navy
TRIAL LOCATIONS: USEUCOM, NSWC Dahlgren, SPAWAR, Australia, New Zealand, UK
TRIAL PARTNERS: IT05.37



WARFIGHTER
TECHNICAL / INTEROPERABILITY
INFORMATION ASSURANCE
SYSTEMS ENGINEERING

ASSESSMEMT RESULTS:
During CWID 2006, the FnDCS Trial received Warfighter, Technical Interoperability, and Information Assurance assessments.

■ FnDCS successfully received raw data tracks, fused them with ambiguous sensor track data and passed them to JEBC2 (its partner). FnDCS did not fully meet Objective 5 since repeated display discrepancies disrupted the commanders maritime picture and impacted the trials overall effectiveness.

■ FnDCS successfully demonstrated CWID Objective 1 using a persistent Universal Chat Client tool that was very functional, easy to use, and became the primary command and control circuit for Navy role players at Dahlgren.

■ A detractor to the trial was that IA scans encountered Trojan signatures on several open ports as well as several other vulnerabilities for the version of SSH, limiting cryptographic transmissions.

GO TO CD HOME PAGE

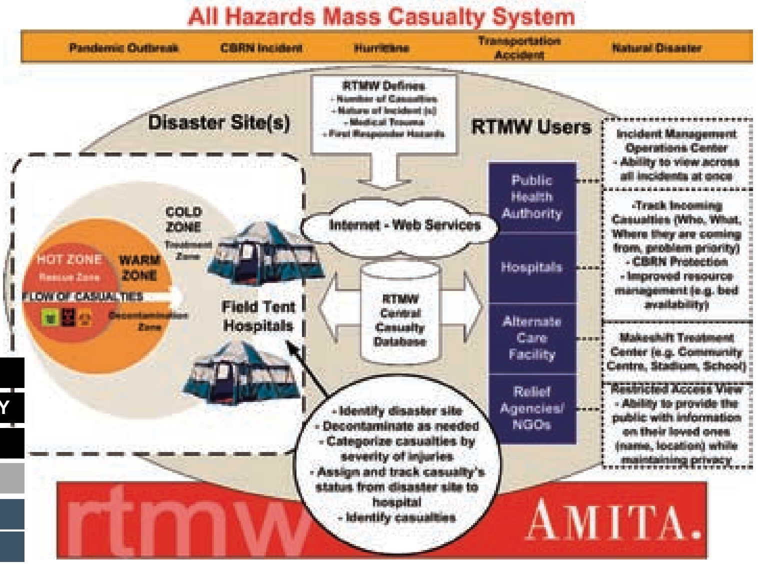
IT05.52

Rapid Triage Medical Workbench

3. INTEGRATED LOGISTICS ● 5. NET CENTRIC ENTERPRISE SERVICES ●

TRIAL OVERVIEW: Rapid Triage Medical Workbench (RTMW) is a software tool for military and civilian front-line emergency responders and medical personnel to collect and share casualty information. RTMW improves emergency care during a mass casualty by providing access to a central source of data for patient tracking including alternate hospital location and medical problem details.

SPONSOR: USNORTHCOM
TRIAL LOCATIONS: USNORTHCOM, NSWC Dahlgren, SPAWAR, Canada
TRIAL PARTNERS: None


All Hazards Mass Casualty System
Pandemic Outbreak
CBRN Incident
Hurricane
Transportation Accident
Natural Disaster
Disaster Site(s)
RTMW Defines
- Number of Casualties
- Nature of Incident (s)
- Medical Trauma
- First Responder Hazards
RTMW Users
Incident Management Operations Center
- Ability to view across all incidents at once
COLD ZONE
Treatment Zone
HOT ZONE
Rescue Zone
WARM ZONE
FLOW OF CASUALTIES
Decontamination Zone
Field Tent Hospitals
Internet - Web Services
RTMW Central Casualty Database
Public Health Authority
Hospitals
Alternate Care Facility
Relief Agencies/ NGOs
-Track Incoming Casualties (Who, What, Where they are coming from, problem priority)
- CBRN Protection
- Improved resource management (e.g. bed availability)
Makeshift Treatment Center (e.g. Community Centre, Stadium, School)
Restricted Access View
- Ability to provide the public with information on their loved ones (name, location) while maintaining privacy
- Identify disaster site
- Decontaminate as needed
- Categorize casualties by severity of injuries
- Assign and track casualty's status from disaster site to hospital
- Identify casualties
rtmw
AMITA.

WARFIGHTER

TECHNICAL / INTEROPERABILITY

INFORMATION ASSURANCE

SYSTEMS ENGINEERING

GO TO CD TRIAL DIRECTORY

GO TO CD HOME PAGE

ASSESSMEMT RESULTS:
During CWID 2006, the RTMW Trial received Warfighter and Technical Interoperability assessments.

■ RTMW successfully demonstrated CWID Objectives 5 and 3.

■ RTMW successfully demonstrated a web-based/browser solution that provided a central data source to track and update patient status during a mass casualty event. Data was entered into and retrieved from the database through a web browser via Transmission Control Protocol/Internet Protocol (TCP/IP) HTTP.

■ RTMW also limited data base access based on users' roles, provided easy viewing and record updating and shared information across local, state and national information boundaries.

■ A user-friendly application, RTMW provided accurate and fast information flow from the simulated disaster area to medical facilities.

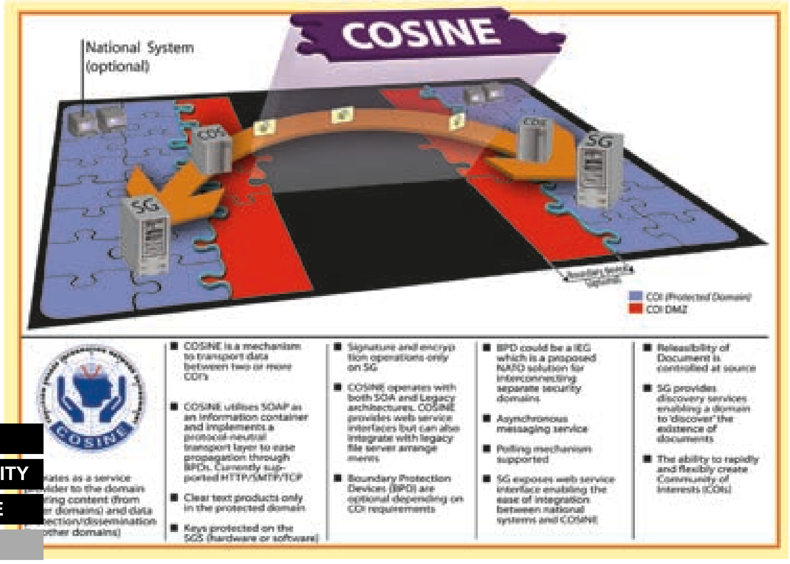
IT05.66

Coalition Shared Information Environment

2. COALITION INFORMATION SHARING ● 5. NET CENTRIC ENTERPRISE SERVICES ●

TRIAL OVERVIEW: Coalition Shared Information Environment (COSINE) facilitates sharing information within a multi-domain, secure, coalition architecture between allied and coalition partners. Based on the COSINE architecture, product control always remains with the data owner/publisher. Users pull documents rather than COSINE pushing documents. This architecture preserves and protects source management functionalities. COSINE facilitates information management and collaboration between interconnected systems. COSINE uses standard Web services technology for inter-process communications and data transfer.

SPONSOR: NATO
TRIAL LOCATIONS: NATO, USEUCOM
TRIAL PARTNERS: None



...ates as a service provider to the domain ...ring content (from ...r domains) and data ...ection/dissemination ...other domains)

■ COSINE is a mechanism to transport data between two or more COI's

■ COSINE utilises SOAP as an information container and implements a protocol-neutral transport layer to ease propagation through BPDs. Currently supported HTTP/SMTP/TCP

■ Clear text products only in the protected domain

■ Keys protected on the SGS (hardware or software)

■ Signature and encryption operations only on SG

■ COSINE operates with both SOA and Legacy architectures. COSINE provides web service interfaces but can also integrate with legacy file server arrangements

■ Boundary Protection Devices (BPD) are optional depending on COI requirements

■ BPD could be a IEG which is a proposed NATO solution for interconnecting separate security domains

■ Asynchronous messaging service

■ Polling mechanism supported

■ SG exposes web service interface enabling the ease of integration between national systems and COSINE

■ Releasibility of Document is controlled at source

■ SG provides discovery services enabling a domain to 'discover' the existence of documents

■ The ability to rapidly and flexibly create Community of Interests (COIs)

WARFIGHTER

TECHNICAL / INTEROPERABILITY

INFORMATION ASSURANCE

SYSTEMS ENGINEERING

ASSESSMEMT RESULTS:
During CWID 2006, the COSINE Trial received Warfighter, and Technical Interoperability assessments.

■ COSINE successfully demonstrated its primary and secondary objectives (2 and 5).

■ Successfully demonstrated Coalition Information Sharing with a planned straightforward approach to data sharing. COSINE provided seamless exchange of information between the NATO Response Force and Coalition Task Force across security boundary devices.

■ COSINE's improved information sharing and synchronization processes allowed users to access, review, and approve intelligence reports as well as permit operators to dynamically control file permissions and hosting.

HISTORY OF CWID

CWID traces more than 16 years of history to establishment of the Secure Tactical Data Network (STDN) series originated by the U.S. Army to demonstrate emerging command, control, communications and computer (C4) capabilities.

STDN 1 and 2 concentrated on Army-only issues while STDN 3 brought the first multi-service participation. The Joint Staff recognized that advances in communications and information technology in the public sector were outpacing Department of Defense (DoD) capabilities.

The Joint Staff assumed sponsorship of the STDN series in 1993 under the C4I for the Warrior concept. The Defense Information Systems Agency (DISA) was directed to be Executive Agent, in concert with a lead Service, to organize network experiments, bringing emerging public sector and other government agency technologies into DoD projects and into war-fighters' sphere of recognition. DISA was also directed to improve joint C4 interoperability.

In 1994, annual STDN efforts evolved into the first Joint Warrior Interoperability Demonstration (JWID). The Air Force was lead service and U.S. Atlantic Command was host combatant command. The idea of moving from a static, one-dimensional picture of the battlefield to a near real-time, multi-dimensional battlespace picture became reality to joint and combined warfighters.

Key efforts in JWID '94 included demonstration of baseline segments of what became the Global Command and Control System (GCCS). Six weeks after the conclusion of JWID '94, GCCS was operationally deployed to U.S. Atlantic Command supporting military operations in Haiti. Full operational deployment of GCCS to all combatant commanders occurred within 12 months after JWID '94.

In 1997, the Chairman of the Joint Chiefs of Staff mandated interoperability in Joint Vision 2010, envisioning future conflicts as coalition operations. JWID assisted that vision, establishing itself as a coalition interoperability forum through invitations to Combined Communications Electronics Board (CCEB) nations (Australia, Canada, New Zealand and the United Kingdom) and NATO beginning with JWID '94 and continuing to the present. While invited participants used JWID to perform their own technology demonstrations and joint interoperability trials, their main intent was to promote and ensure C4 interoperability with the U.S.

EXPANSION

In 1998, JWID evolved into a two-year process to pursue selection and limited fielding of C4 technologies to warfighting combatant commanders. The Theme (first) Year conducted demonstrations and interoperability trials and selected "Gold Nuggets" for support and continued improvement during the Exploitation (second) Year, with eventual fielding to combatant commands. JWID '98 fielded three Gold Nuggets to warfighters.

U.S. Y2K concerns drove JWID '99-R to focus only upon coalition interoperability trials between the U.S. and CCEB/NATO nations.
To more easily promote trials and other Command, Control, Communications, Computers and Intelligence (C4I) experiments, the Coalition Wide Area Network (CWAN), established annually for JWID, evolved into the standing Combined Federated Battle Laboratories Network (CFBLNet). The network permits C4I experimentation among the U.S. and nations of CCEB/NATO year-round, using systems jointly owned and managed by CFBL membership.

JWID '00-'01 restored the two-year cycle, with 23 U.S. demonstrations and 145 combined/coalition demonstrations worldwide. Two Gold Nuggets were fielded in 2001. In addition, a Distributed Collaborative Tool Set (DCTS, now Defense Collaboration Tool Suite) was refined and subsequently selected for worldwide fielding to the Unified Commands. DISA fielded the capability, within 72 hours, in support of the Office of the Secretary of Defense (OSD) requirements following terrorist attacks of September 11th, to multiple DoD networks.

COALITION INTEROPERABILITY

JWID 2002 featured transition from a limited fielding of technology to full focus on coalition interoperability, led by U.S. Pacific Command (USPACOM), the host combatant command. The demonstration included Pacific Rim nations in a Pacific Theater Initiative (PTI), with Japan, South Korea, Singapore, and Thailand participating while Malaysia and the Philippines observed operations. Coalition partners were integrated on the Multinational Task Force (MTF) and component staffs to maximize opportunities. The JWID CWAN continued use of CFBLNet architecture and services established in past demonstrations. U.S. Joint Forces Command (USJFCOM) fielded a JWID demonstrated language translation device.

JWID 2003 took coalition interoperability to new heights. USPACOM guided the CTF and, for the first time, Japan, South Korea, Thailand and Singapore provided staffing to expand information exchange over dual domains. One key focus for 2003 included management of information exchange between the traditional 6-eyes network to a larger, more robust 10-eyes network. The larger network was vital to JWID's success because Pacific Rim nations needed effective information to serve in MTF staff positions. JWID 2003 addressed multi-level security technical solutions and refinement of coalition policies and procedures to overcome issues surrounding information exchange.

DISA assumed duties as the lead agency, providing broad-base management support of JWID activities. Four Coalition Interoperability Trials (CITs) with especially noteworthy performance were submitted to USJFCOM J861, for consideration for limited fielding.

HOMELAND SECURITY

JWID 2004 featured U.S. Northern Command (USNORTHCOM) as the Host Combatant Command. USNORTHCOM brought a Homeland Security/Homeland Defense (HLS/HLD) focus to the demonstration. This approach broke new ground beyond the traditional JWID coalition interoperability area, adding government interagency information sharing. USNORTHCOM, in a departure from previous JWIDs, invited agencies within the Department of Homeland Security, including first-time participation for the Federal Emergency Management Agency (FEMA), the Federal Bureau of Investigation (FBI), the U.S. Coast Guard, and the National Guard Bureau. Limited coalition participation between these organizations occurred as Canada's Office of Critical Infrastructure Protection joined in the interoperability trials. This activity offers significant potential for more extensive cooperation between other coalition homeland security organizations and their U.S. counterparts. USJFCOM filled an ancillary role, assisting with select fielding of technologies to combatant commanders. JWID 2004 involved 25 countries, military services, and government agencies participating in a scripted scenario over a global network.

USNORTHCOM was host Combatant Command in 2005 as the demonstration moved forward with a name change. Now the Coalition Warrior Interoperability Demonstration (CWID), the shift from "Joint" to "Coalition" describes the larger community of participants, including national and international government agencies. A new name was not the only change for CWID in 2005.

USJFCOM formally assumed oversight for planning and execution of CWID 2005 from the Joint Staff in July 2004. This involvement brings USJFCOM advocacy for U.S. combatant command interoperability shortfall resolution to the forefront. USJFCOM's objectives include (1) to ensure CWID demonstrates relevant technologies that address combatant commander's capability gaps, (2) to investigate military, coalition and interoperability solutions and (3) to identify technologies suitable for prototype initiatives.

CWID 2005 featured revitalization of the planning and collaboration web site, including readily accessible general information. Online trial submission abbreviated initial proposal processes for interested technology representatives. Additionally, CWID established a Concept of Operations (CONOPs) for all recurring aspects of planning and execution.

The CWID 2005 Execution results were noteworthy in that most ITs successfully achieved their stated objectives. More than 400 operators from the military and supporting agencies, at multiple U.S. and coalition sites, executed the scenario events to evaluate and report on trial performance.

Fifteen trials were considered "success stories," moving forward for continued development. Seven ITs were selected for Service, Agency, or limited Combatant Commander fielding (including fielding in support of Hurricane Katrina). Two ITs achieved milestones and continue spiral development as Programs of Record. One was selected for funding via a Congressional Plus-up for further research and development, and one was submitted as a Limited Acquisition Authority candidate. Four others were identified for agency fielding in some capacity.

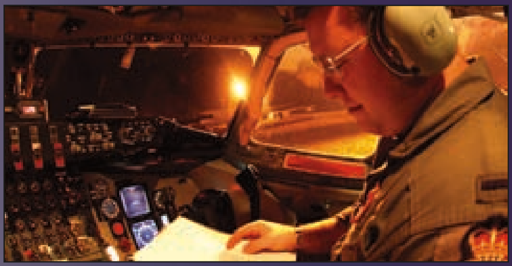
U.S. European Command (USEUCOM) is the host combatant command for 2006 through 2008. USNORTHCOM continues as the lead for HLS/HLD CWID operations.

GO TO CD HOME PAGE

Abbreviations and Acronyms

ACO	Airspace Control Order
ACT	Allied Command Transformation
ATM	Asynchronous Transfer Mode
ATO	Air Tasking Order
AWG	Assessment Working Group
C2	Command and Control
C2I	Command and Control Information
C2IS/CCIS	Command and Control Information System
C3	Command, Control, Communications
C3	Consultation, Command and Control
C4	Command, Control, Communications, and Computers
C4I	Command, Control, Communications, Computers and Intelligence
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CAC	Common Access Card
CAOC	Combined Air Operations Center
CBRN	Chemical, Biological, Radiological, Nuclear
CCCC	Combined Communications Control Center
CCEB	Combined Communications-Electronics Board
CFBLNet	Combined Federated Battle Laboratories Network
CIS	Computer Information Systems
CND	Computer Network Defense
CNR	Combat Net Radios
COI	Communities of Interest
COMSEC	Communications Security
CONOPS	Concept of Operations
COP	Common Operational Picture
C/S/A	Combatant Commands, Services, and Agencies
CTF	Coalition Task Force
CWAN	Coalition Wide Area Network
CWID	Coalition Warrior Interoperability Demonstration
CWID JMO	CWID Joint Management Office
DCTS	Defense Collaboration Tool Suite
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DISN-LES	Defense Information Systems Network - Leading Edge Services
DoD	Department of Defense
DTRA	Defense Threat Reduction Agency
FBI	Federal Bureau of Investigation
FBO	Federal Business Opportunities
FEMA	Federal Emergency Management Agency
GBS	Global Broadcast System
GCCS	Global Command and Control System
GIG	Global Information Grid
GIS	Geographical Information System
GPS	Global Positioning System
GWOT	Global War on Terrorism
HF	High Frequency
HLS/HLD	Homeland Security/Homeland Defense
IA	Information Assurance
ICC	Integrated Command and Control
IER	Interface Exchange Requirement
IP	Internet Protocol
IPC	Initial Planning Conference
ISP	Internet Service Provider
IT	Interoperability Trial
JDCAT	JSIC Data Collection Analysis Tool
JFHQ	Joint Forces Headquarters
JIEE	Joint Information Exchange Environment
JITC	Joint Interoperability Test Command
JSIC	Joint Systems Integration Command
JWID	Joint Warrior Interoperability Demonstration
LAN	Local Area Network
LCCIS	Land Command and Control Information System
Mbps	Megabits per second
MCCIS	Maritime Command and Control Information System
MCM	Mine Countermeasures
MNIS-JPO	Multinational Information Sharing - Joint Program Office (DISA)
MOP	Measures Of Performance
MSEL	Master Scenario Events List
MTF	Message Text Format
MTF	Multinational Task Force
NATO	North Atlantic Treaty Organization
NC3A	NATO Consultation Control and Consultation Agency
NNEC	NATO Network Enabled Capability
NIPRNET	Non-Secure Internet Protocol Router Network
NGO	Non-Governmental Organization
NRF	NATO Response Force
NSA	National Security Agency
OSD	Office of the Secretary of Defense
OTH	Over The Horizon
PATM	Public Asynchronous Transfer Mode
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
PTI	Pacific Theater Initiative
RFI	Request for Information
RMP	Recognized Maritime Picture
SA	Situational Awareness
SEIWG	Systems Engineering and Integration Working Group
SMG	Senior Management Group
SPOW	Scientific Programme of Work (NATO)
STDN	Secure Tactical Data Network
TBMCS	Theatre Battle Management Core System
TCP	Transmission Control Protocol
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WICAT	WISE Interoperability Collection and Management Tool
WiFi	Wireless Fidelity
WISE	Web Information Services Environment
XML	Extensible Markup Language

GO TO CD HOME PAGE



2007 Objectives

For more detailed objective explanations and additional information regarding CWID 2007, refer to the Federal Business Opportunities (FBO) and other resources on the demonstration website.

OBJECTIVE 1

CROSS-DOMAIN DATA SHARING

■ Provide the capability to share information across multiple networks of potentially different security classifications and caveats.

OBJECTIVE 2

INTEGRATED INTELLIGENCE

■ Provide solutions that improve the commander's ability to share intelligence information products (documents, images, databases, etc.) with coalition partners, including joint and coalition forces, government agencies, Non-Government Organizations (NGOs) and first responders.

OBJECTIVE 3

INTEGRATED OPERATIONS

■ Enhance the commander's capability to command, control and coordinate across joint and coalition forces, government agencies, NGOs, and first responders.

OBJECTIVE 4

INTEGRATED LOGISTICS

■ Demonstrate the ability to access and consolidate logistical information across organizational boundaries to provide the ability to assess and display, in near real time, information on the movement, location and status of joint forces, military services, interagency, coalition, NGO and first responder equipment, supplies and personnel en route, and/or deployed.

OBJECTIVE 5

INTEGRATED PLANNING

■ Provide solutions that improve the combatant commander's ability to conduct collaborative planning with coalition partners, including joint and coalition forces, government agencies, NGOs and first responders. Focus on enhanced collaboration and engendering a 'need to share' vice a 'need to know' culture.

OBJECTIVE 6

INTEGRATED COMMUNICATIONS

■ Enhance coalition information and knowledge sharing capabilities among Allied, coalition partners, and other bandwidth disadvantaged users, focusing on a robust, joint and combined, interoperable and multi-lingual information sharing capability.

www.cwid.js.mil

GO TO CD HOME PAGE